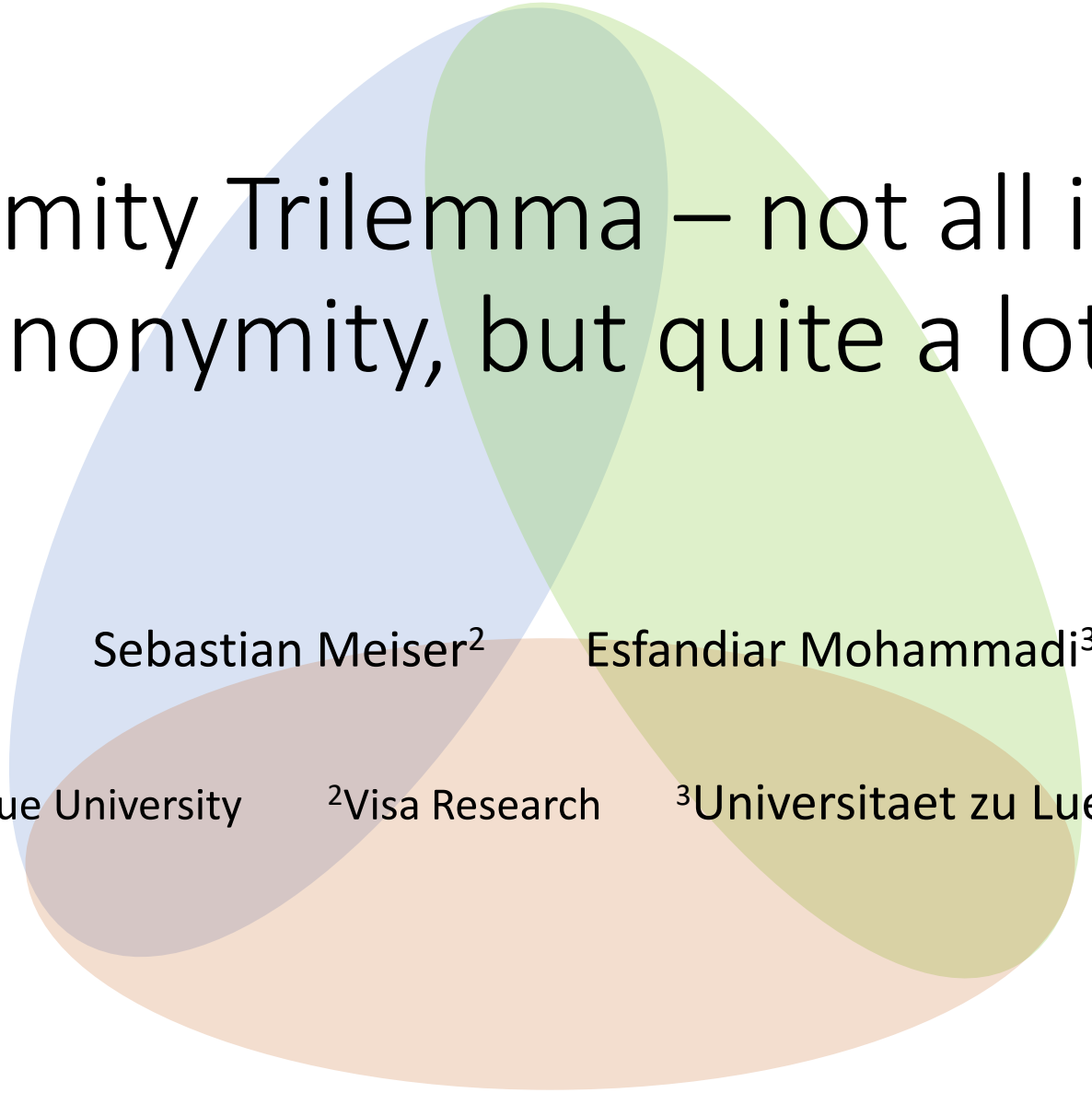
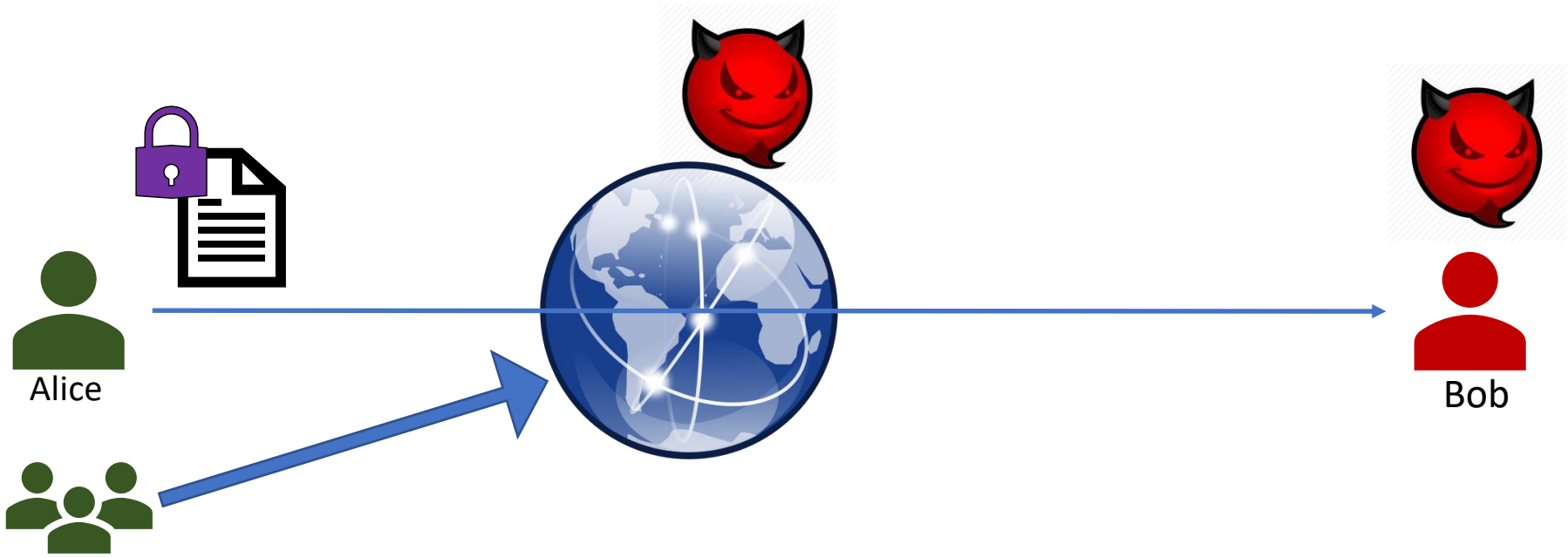
Anonymity Trilemma – not all is lost for anonymity, but quite a lot is.



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

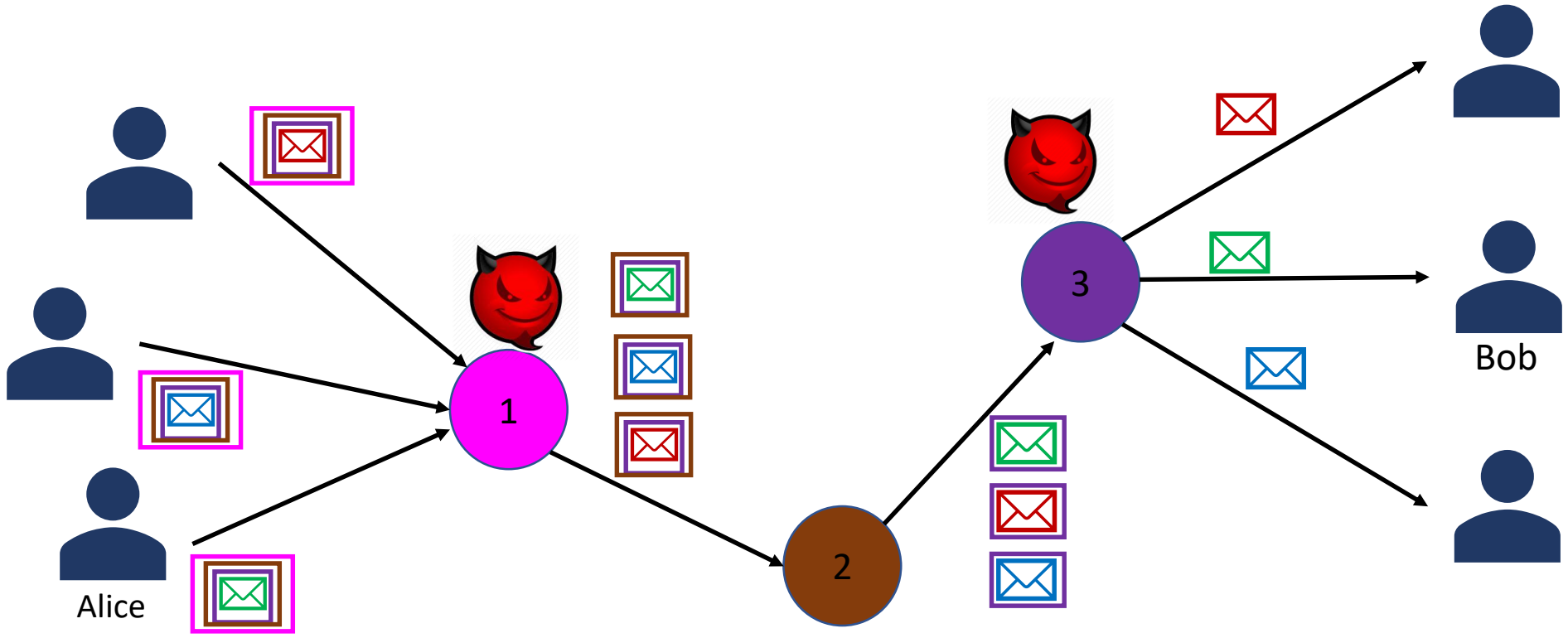
[1]Purdue University [2]Visa Research [3]Universitaet zu Luebeck

Anonymous Communication (AC) Networks



Sender Anonymity

Example AC protocol : Mixnets

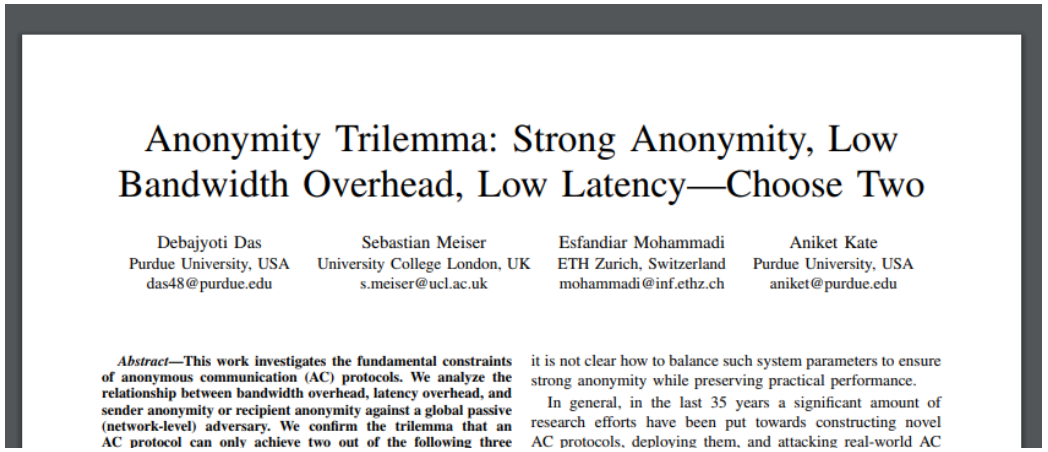


Mixnets can provide anonymity at the cost of high latency overhead.

Anonymity can also be achieved at the cost of high bandwidth overhead.

Anonymity Trilemma

- Q1: Can we achieve good 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

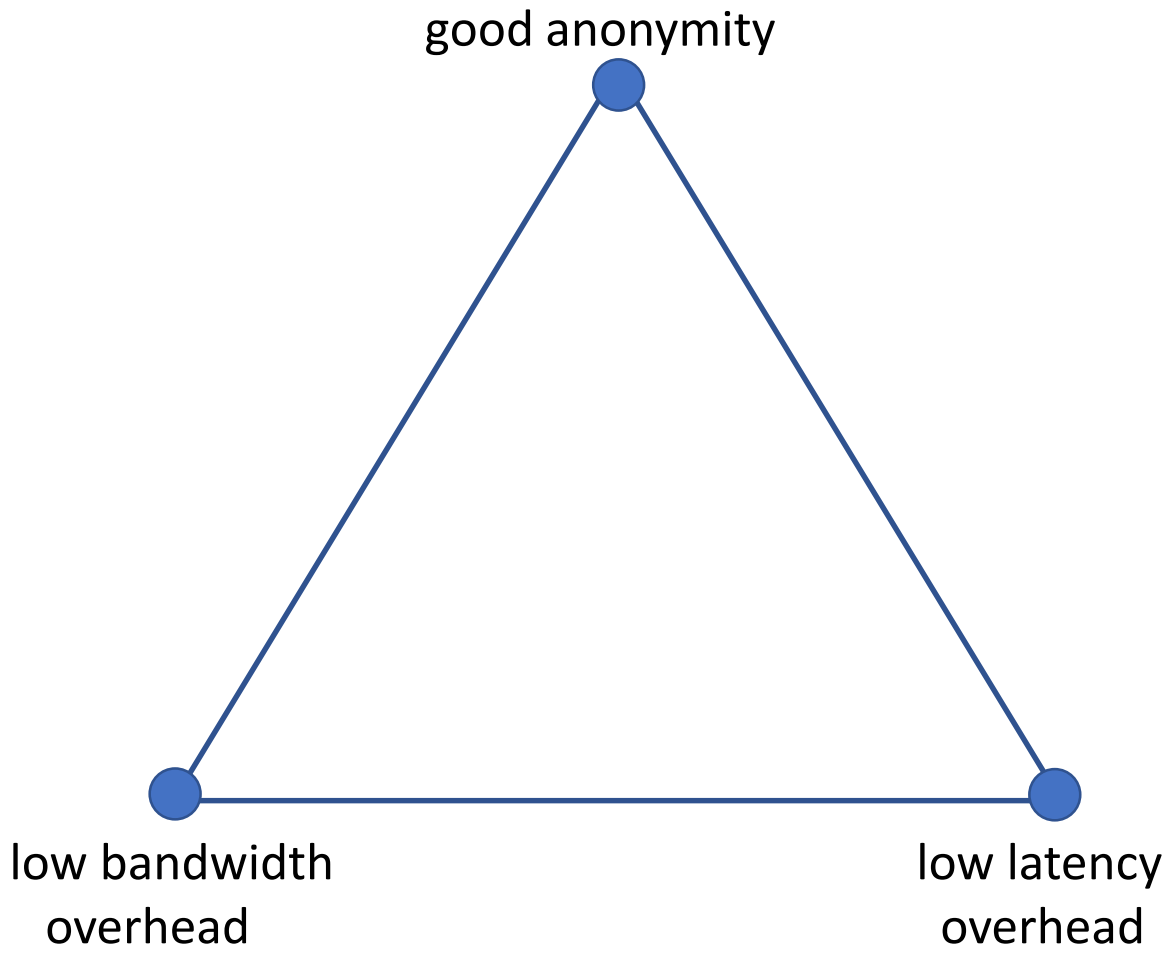
Aniket Kate
Purdue University, USA
aniket@purdue.edu

***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.

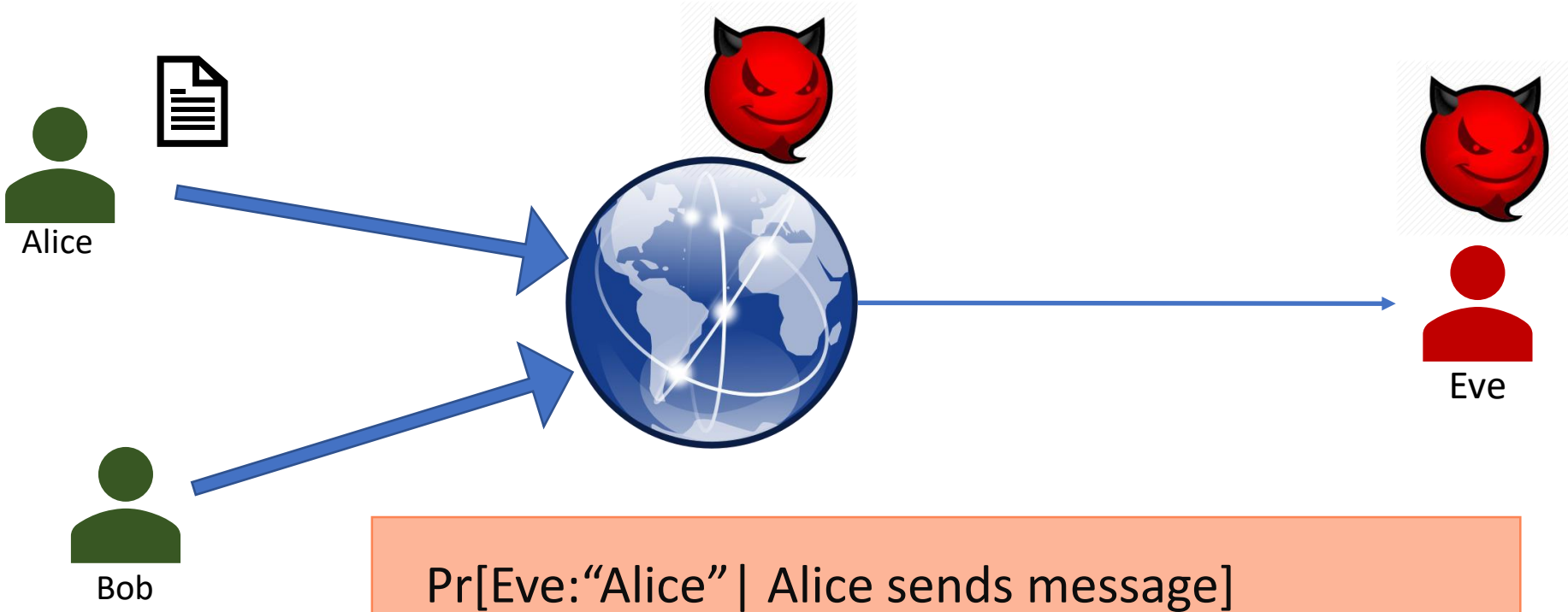
In general, in the last 35 years a significant amount of research efforts have been put towards constructing novel AC protocols, deploying them, and attacking real-world AC

IEEE S&P 2018



strong

Sender Anonymity (AnoA definition)

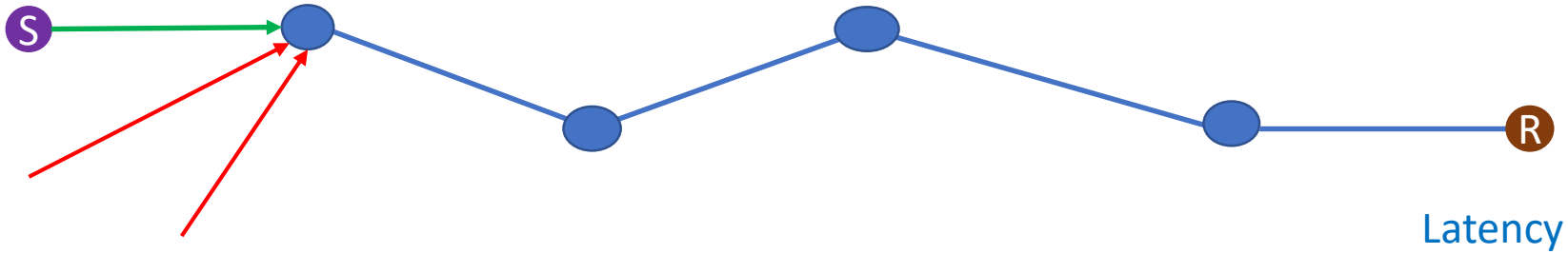


$$\Pr[\text{Eve:“Alice”} \mid \text{Alice sends message}] \leq \Pr[\text{Eve:“Alice”} \mid \text{Bob sends message}] + \delta(\eta)$$

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

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 $\ell = 4$

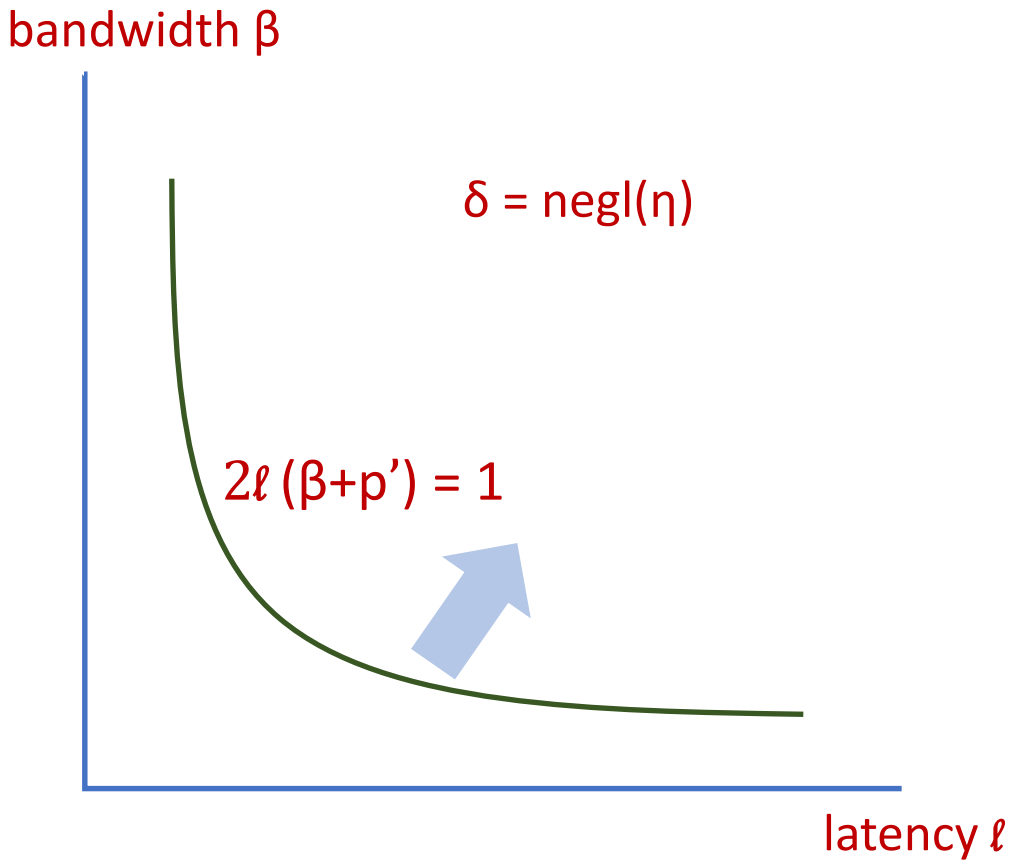
Bandwidth overhead $\beta = 2/4$, $B = 2$

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

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 against a *global passive* adversary:

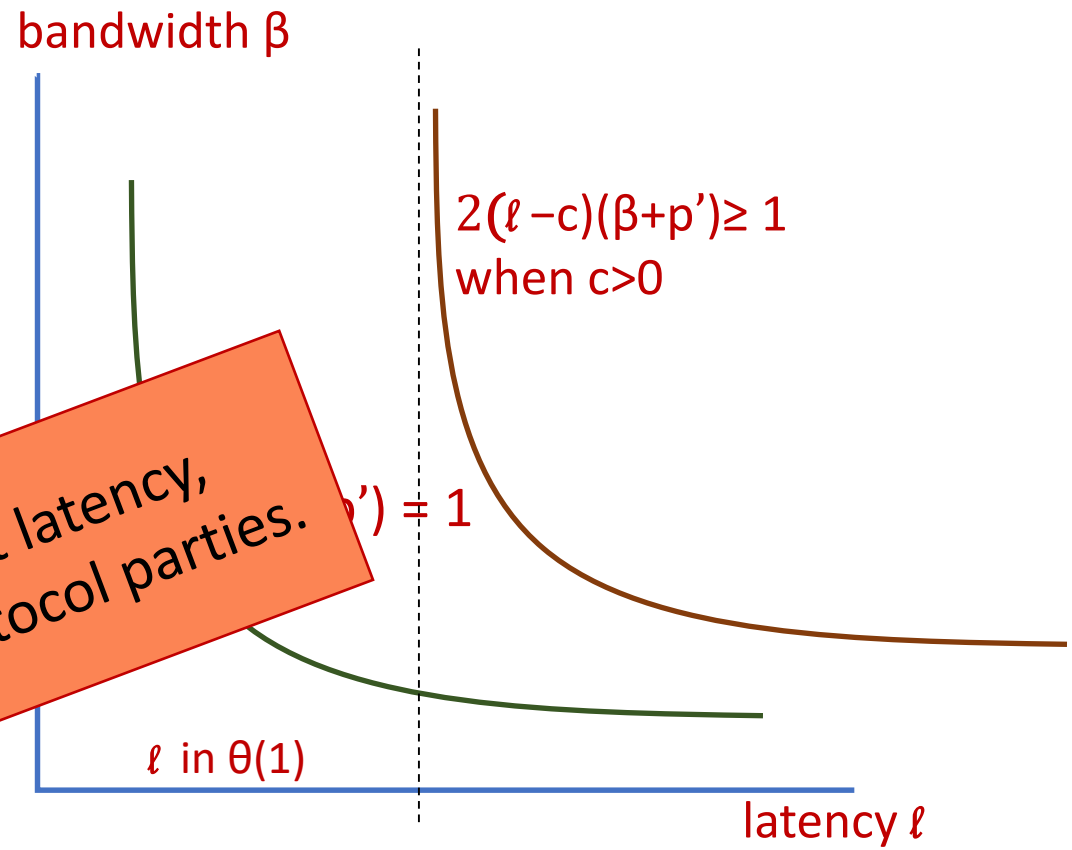
$$2\ell\,(\beta+p') \geq 1$$



When Adversary can compromise c protocol parties

- to achieve strong anonymity against a *passively compromising* adversary:

- $\ell > \theta(1)$
- $2(\ell - c)(\beta + p') \geq 1$, wh



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** ?

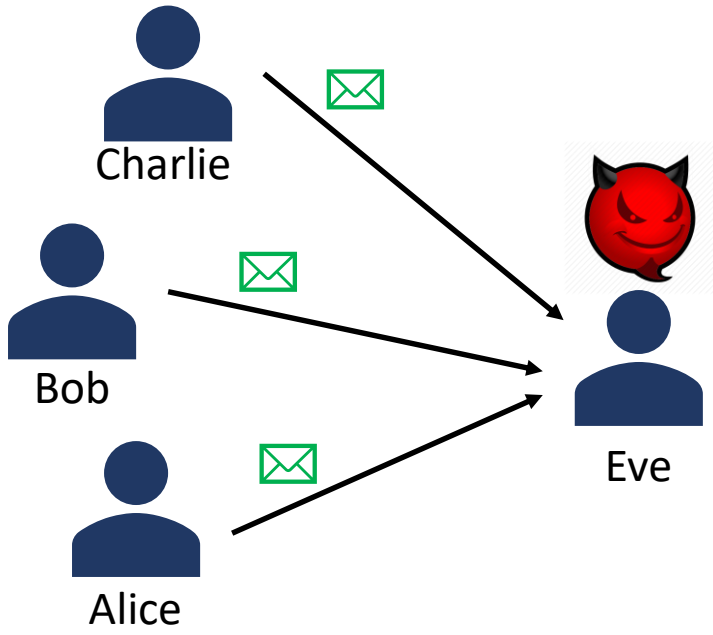
- NO.
- Example: DC-net with **user coordination**.

The protocol model in the previous work did not assume any out-of-band user coordination.

DC-net type protocols – user coordination (UC)

- Alice wants to send *message* m.
- Bob and Charlie send *packets* to help Alice.
- Those 3 packets are *shares* of message m.

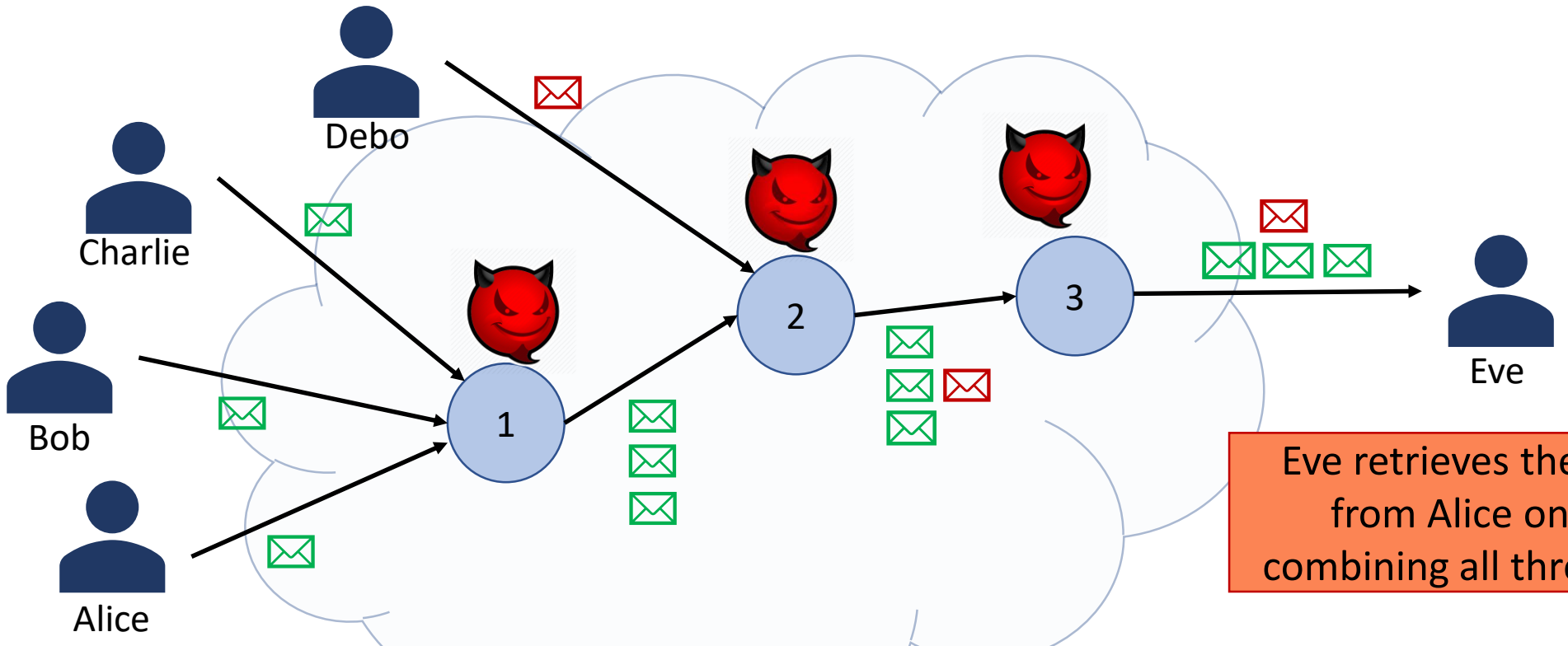
- We assume that this coordination can be achieved via a pre-setup, and hence, the cost of UC to be 0.



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.

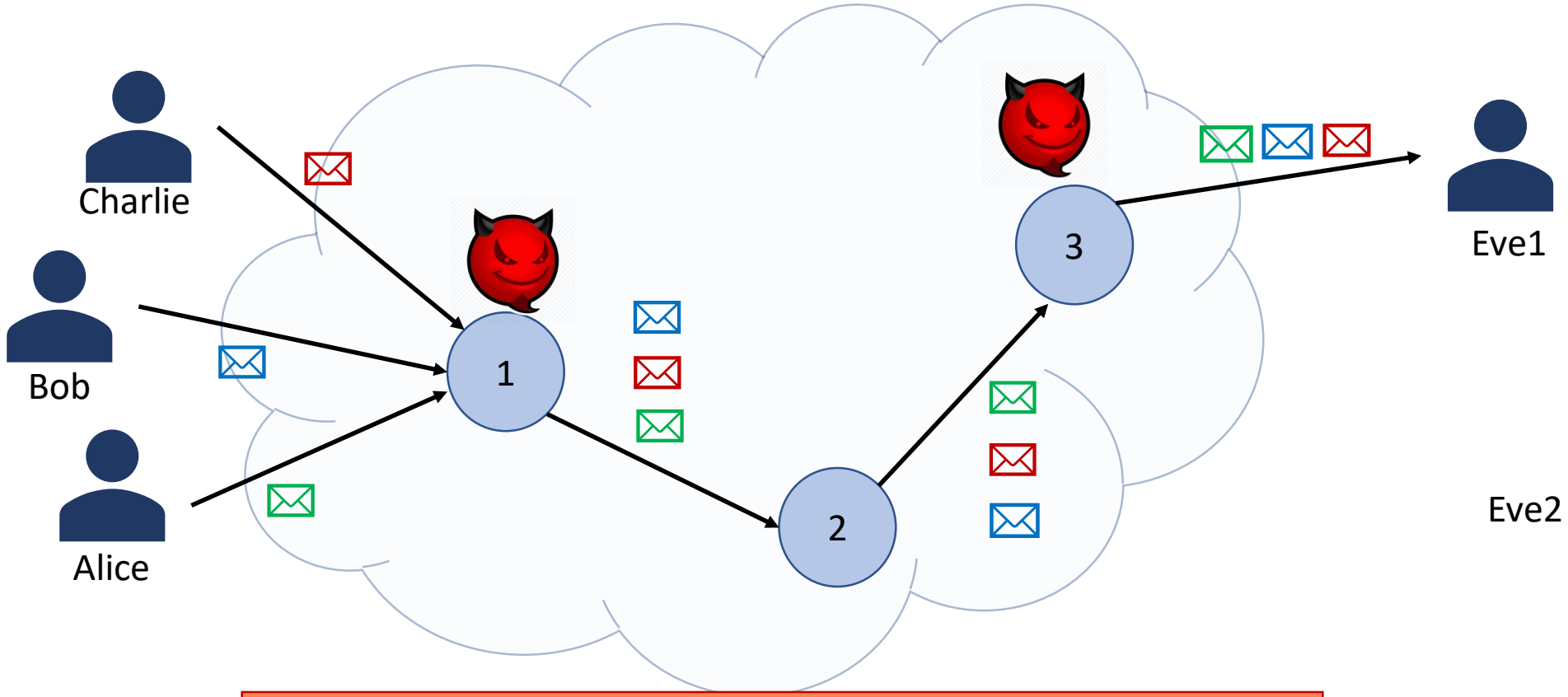
Protocols beyond mix-nets – protocols with UC



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

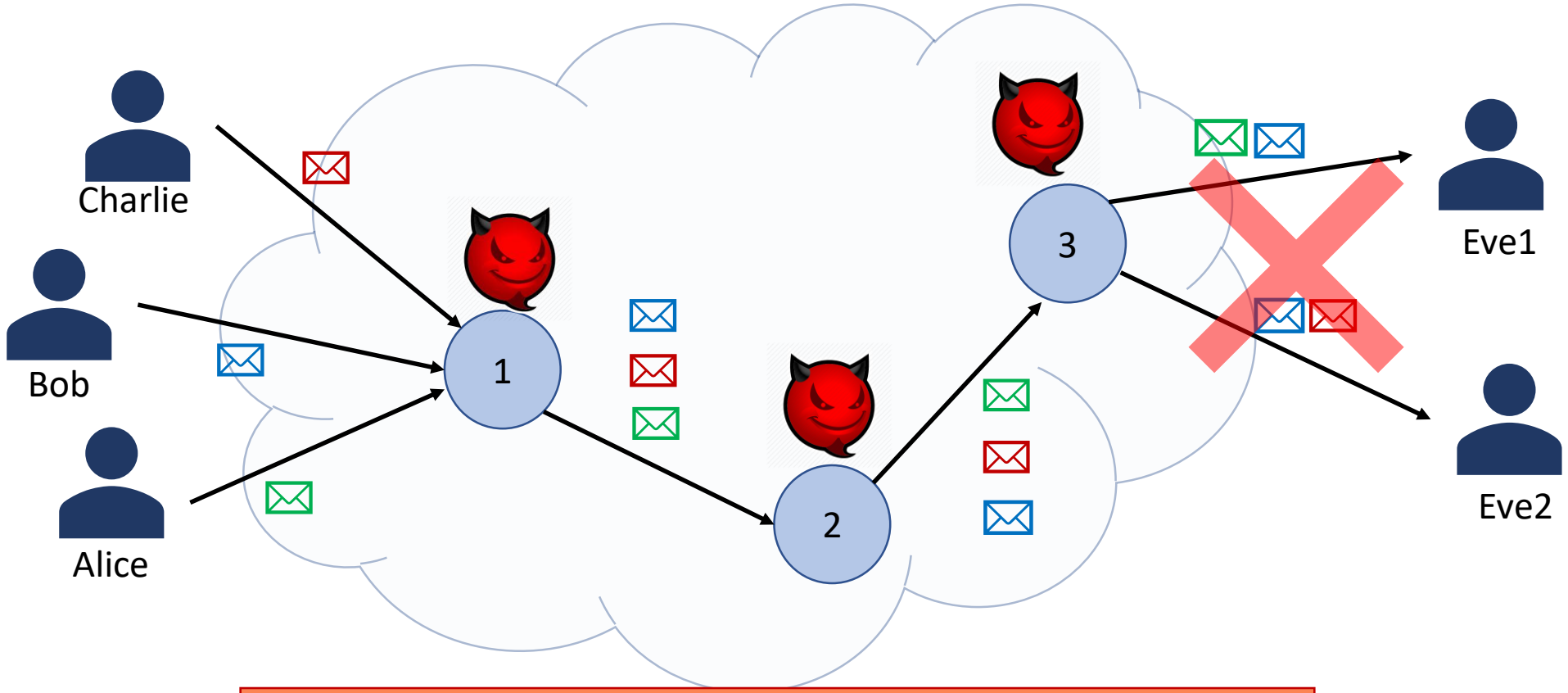
Eve retrieves the message from Alice only after combining all three packets.

Assumptions on protocols with UC



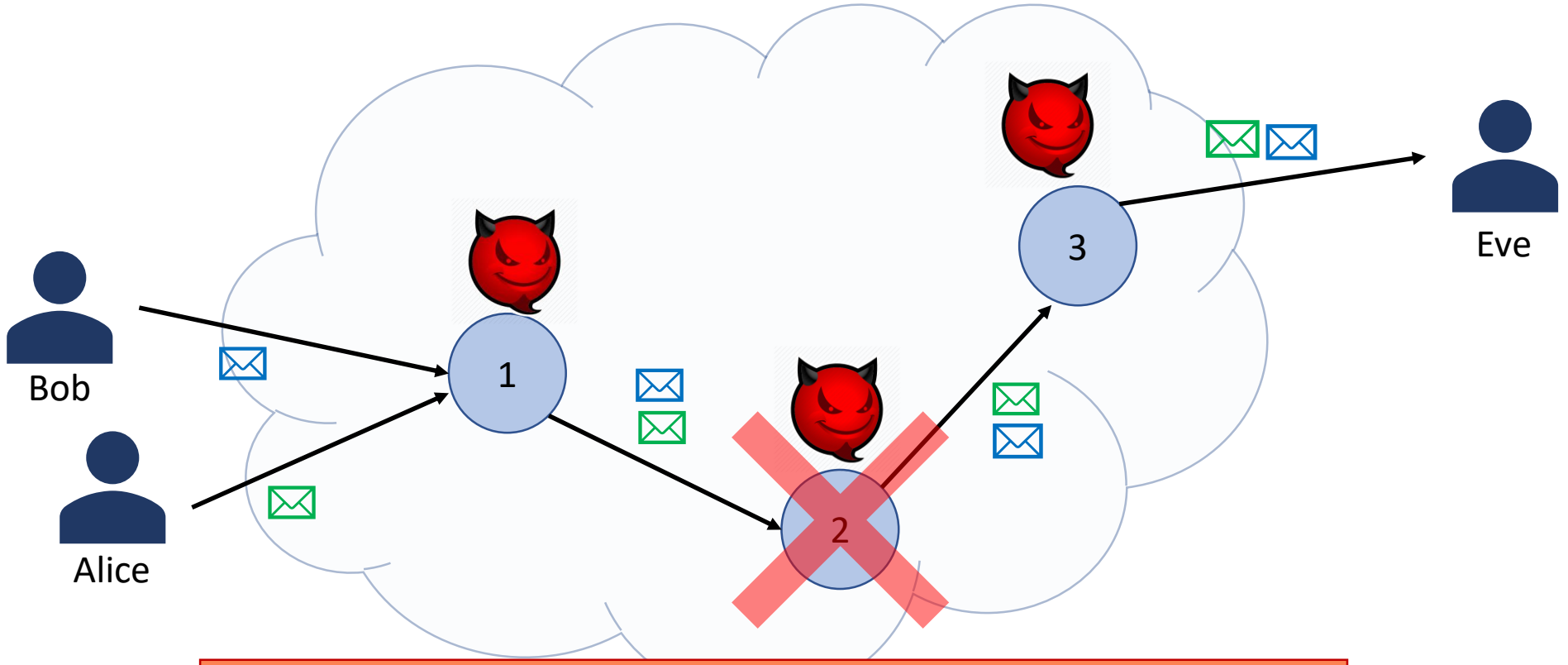
Assumption 1: One of the packets is sent by the actual sender Alice.

Assumptions on protocols with UC



Assumption 2: One packet does not take part in the reconstruction of two separate messages.

Assumptions on protocols with UC

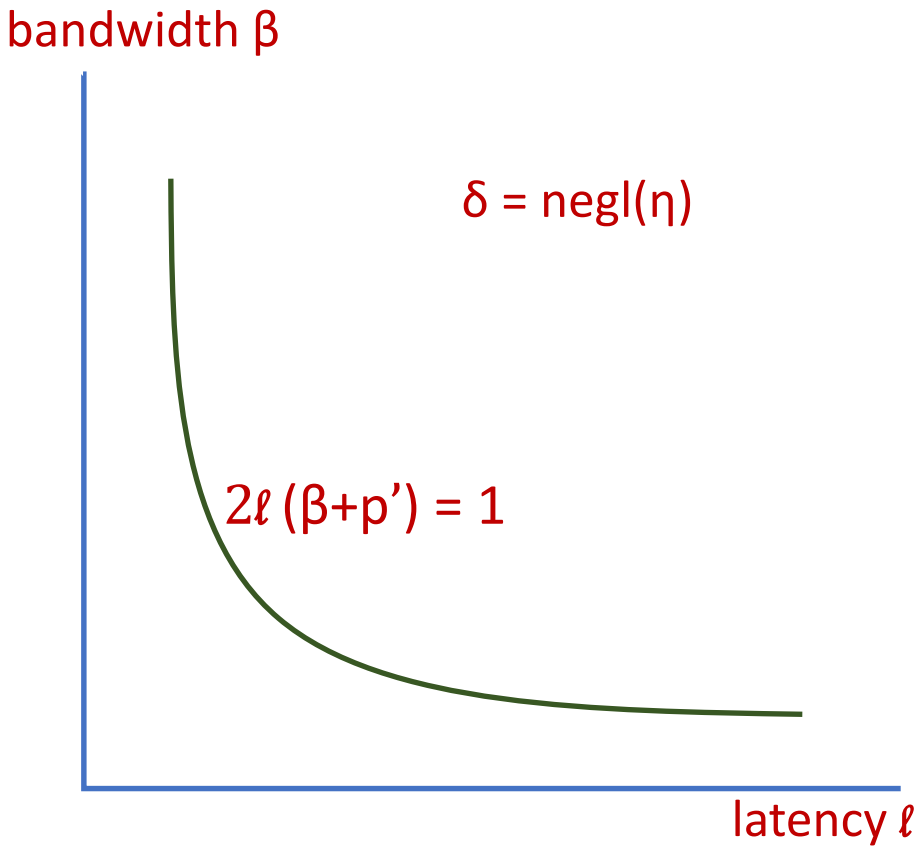


Assumption 3: Mixing is not possible at a compromised node.

Results are same when no parties are compromised

- To achieve strong anonymity against a global passive adversary:

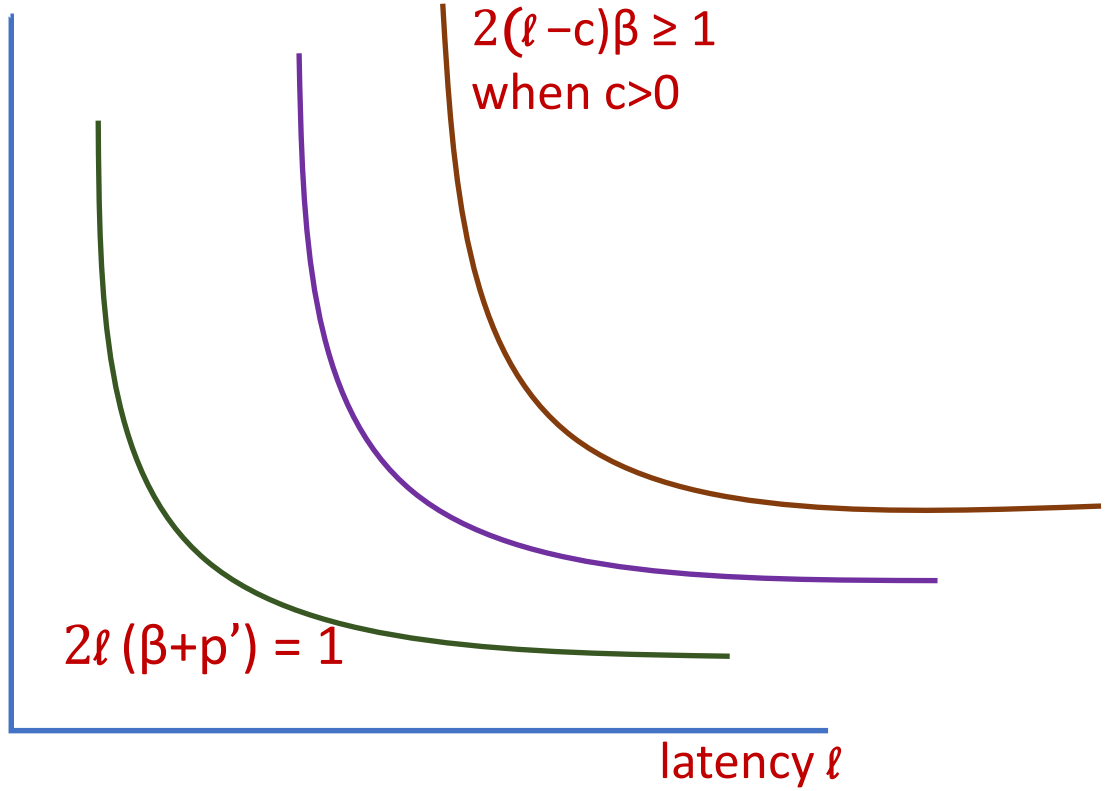
$$2\ell\,(\beta+p') \geq 1$$



The universal necessary constraint still holds, except $\ell = 0$.

Quantum of Solace: when protocol parties are compromised

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



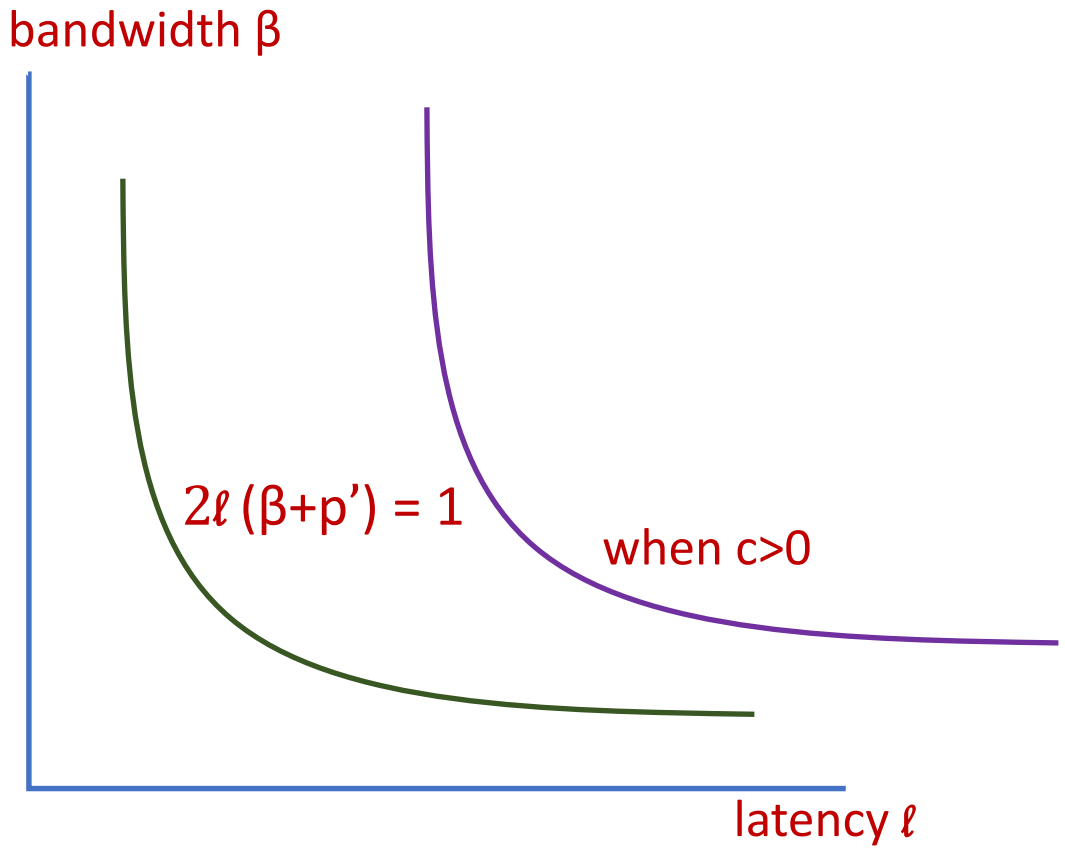
Effect of coordination: resistance against compromised protocol parties – some cases

- Case 1: K/c = const. where K is the total number of nodes.
  The impossibility condition for anonymity:
  - without User Coordination $\ell \in O(\log(\eta))$
  - with User Coordination $\ell^2 \in O(\log(\eta))$

- Case 2: AnyTrust Systems: K-c = const. , $\ell\,\beta=1$, $\ell < c < \ell^2$:
  - it is impossible to achieve strong anonymity for protocols without User Coordination
  - protocols with user coordination escapes that impossibility.

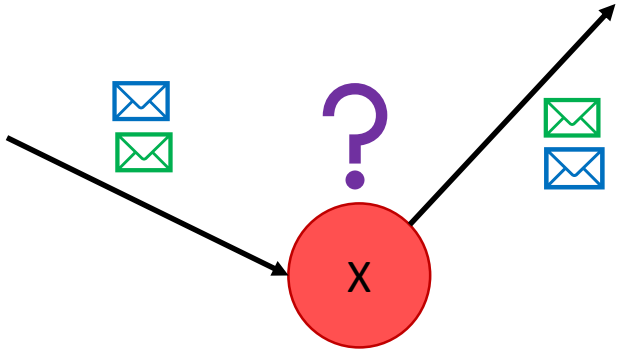
Takeaways

- Our work points protocol designers to focus on protocols with user coordination, to at least achieve resistance against compromization.
- Still we can not do better than the limit specified by the universal necessary constraint: $2\ell\,(\beta+p') \geq 1$.
- Unless we break one of the assumptions on user coordination.



A New Hope:

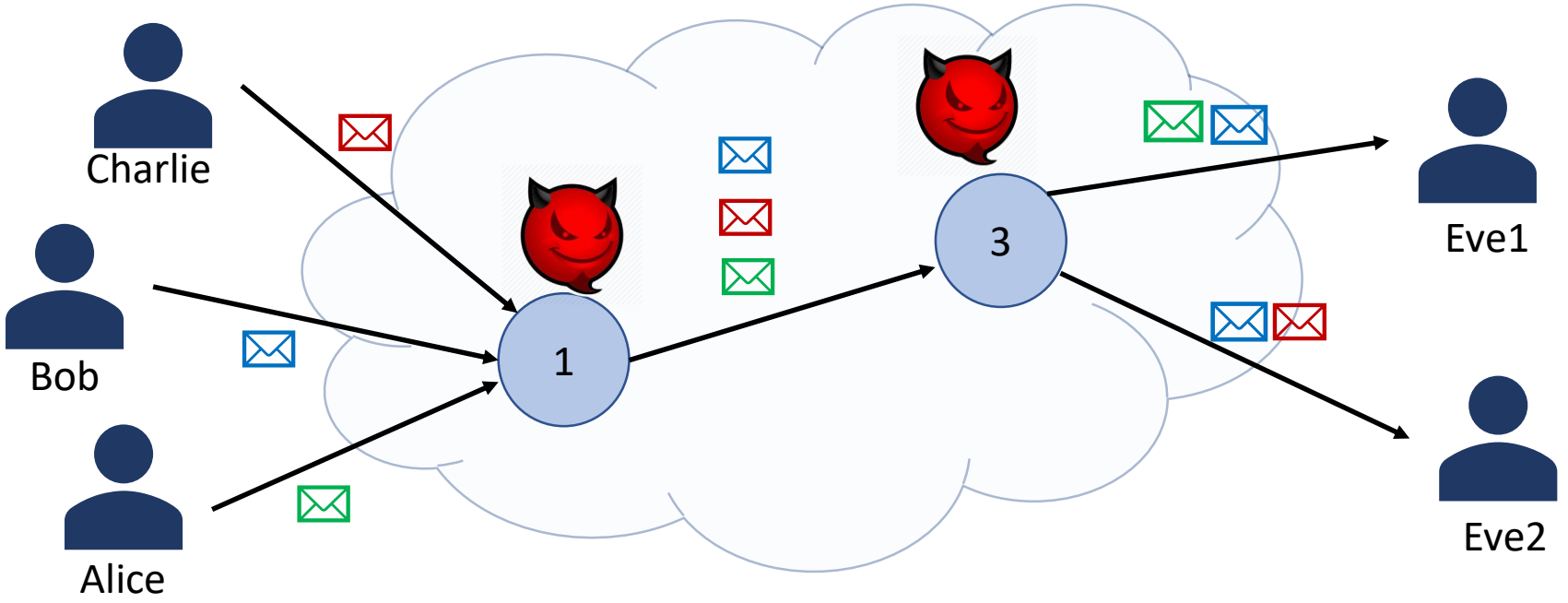
Challenge 1: Achieve mixing at a dishonest node.



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

The Rise of User Coordination:

Challenge 2: Break Assumption 2.
- Generate n shares for m messages in a privacy preserving way with low communication overhead and low latency overhead.



https://freedom.cs.purdue.edu/projects/trilemma.html

Thank you. ☺

 @tutaidas

 das48@purdue.edu