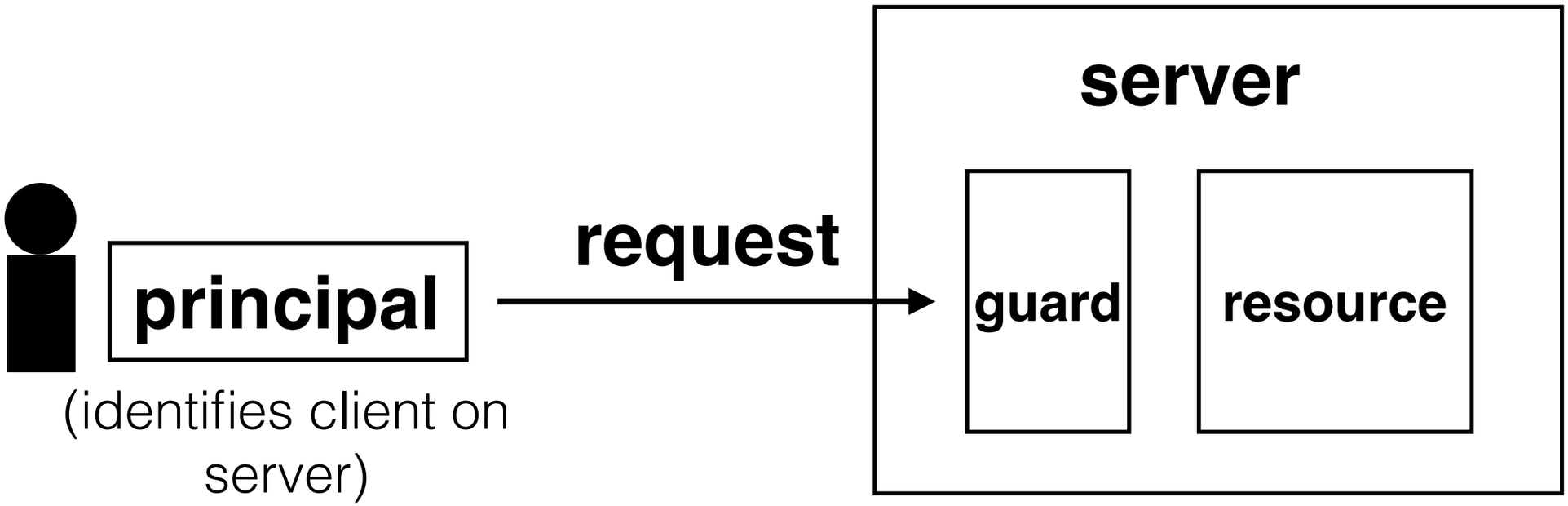
6.033 Spring 2015

Lecture #25

- **Underground web technologies**
  - **Tor**
  - **Digital currency (e.g., Bitcoin)**

Previous Lectures



Tor and Bitcoin

two “underground web technologies” that deal, either directly or somewhat-tangentially, with **anonymity**

Katrina LaCurts | lacurts@mit | 6.033 2015

first, a cryptography review

how to keep data confidential

Katrina LaCurts | lacurts@mit | 6.033 2015

Tor's goal

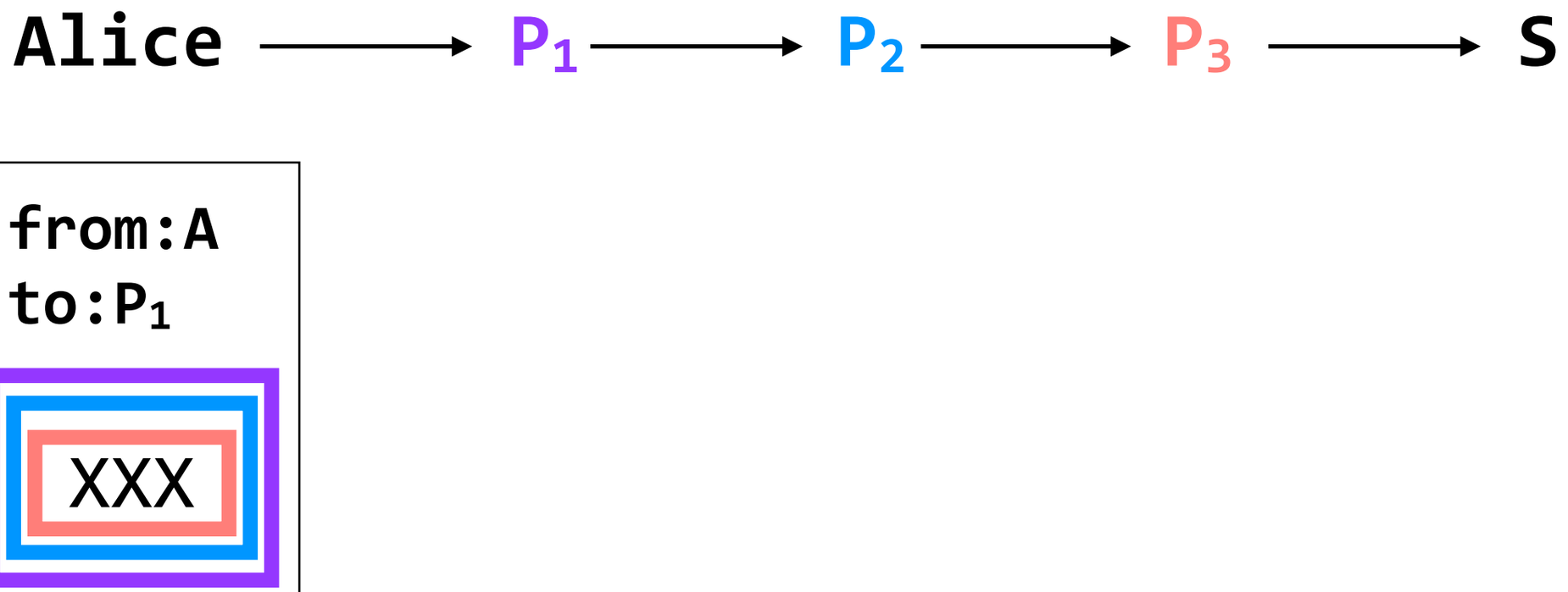
provide **anonymity** — only Alice should know that she is communicating with the server S

Tor's goal

provide **anonymity** — only Alice should know that she is communicating with the server S

things to avoid

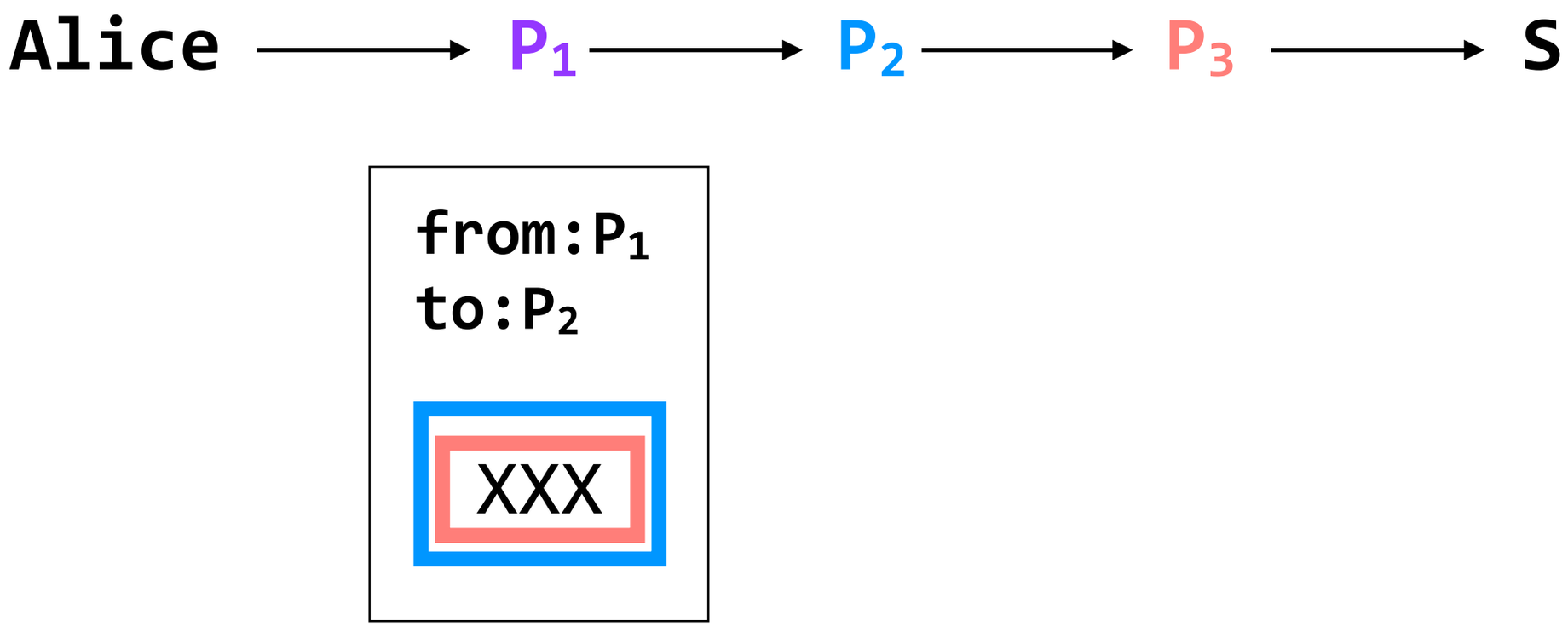
- no packet should say "from: Alice, to: S"
- no entity in the network should receive a packet from Alice and send it directly to S
- no entity in the network should keep state that links Alice to S
- data should not appear the same across multiple packets



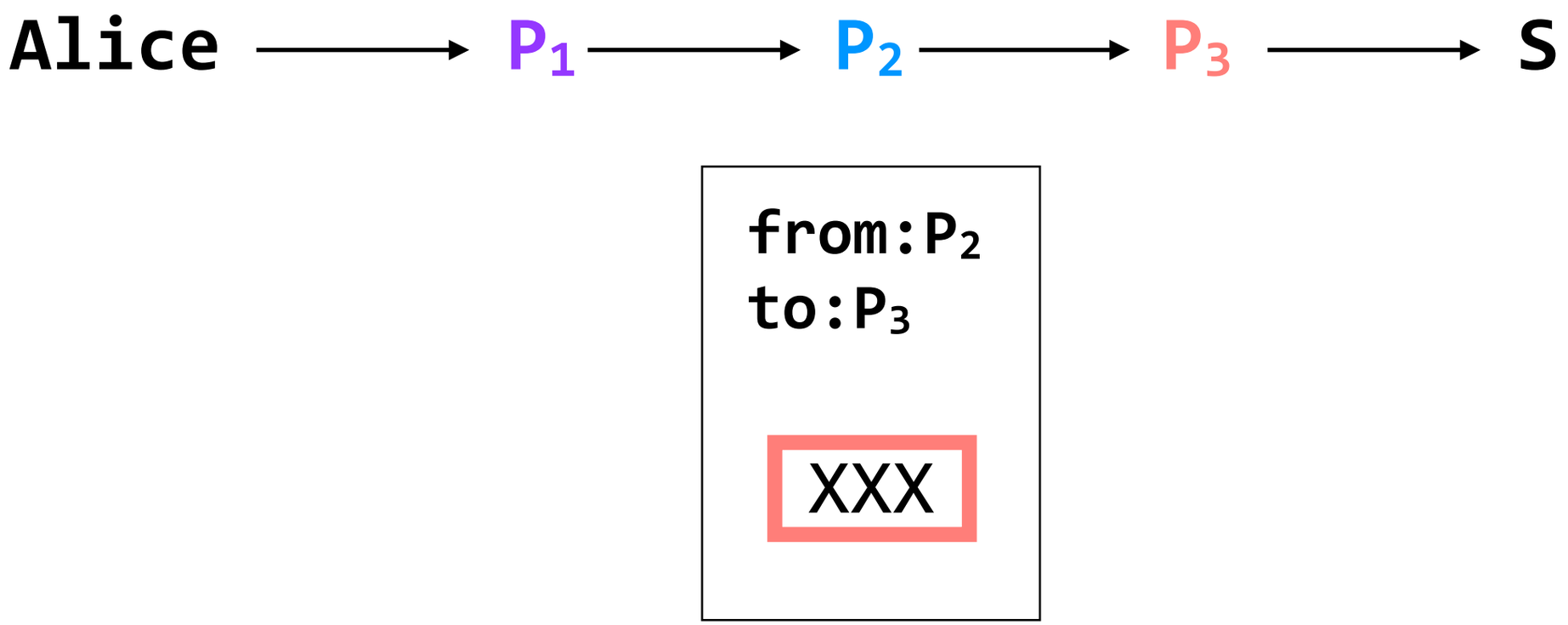
(the circuit ID would also be included and encrypted)

1. Alice adds layers of encryption to her packet

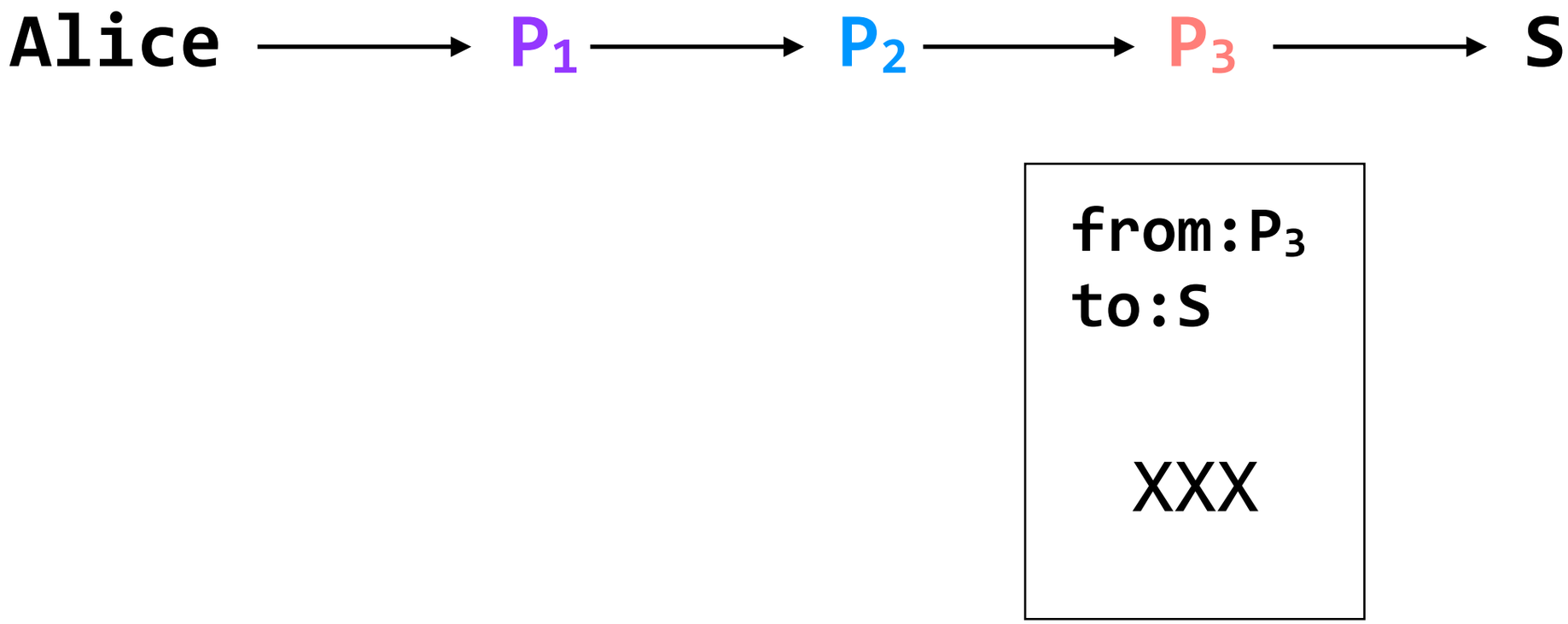
= encrypted with P_3's public key, etc.



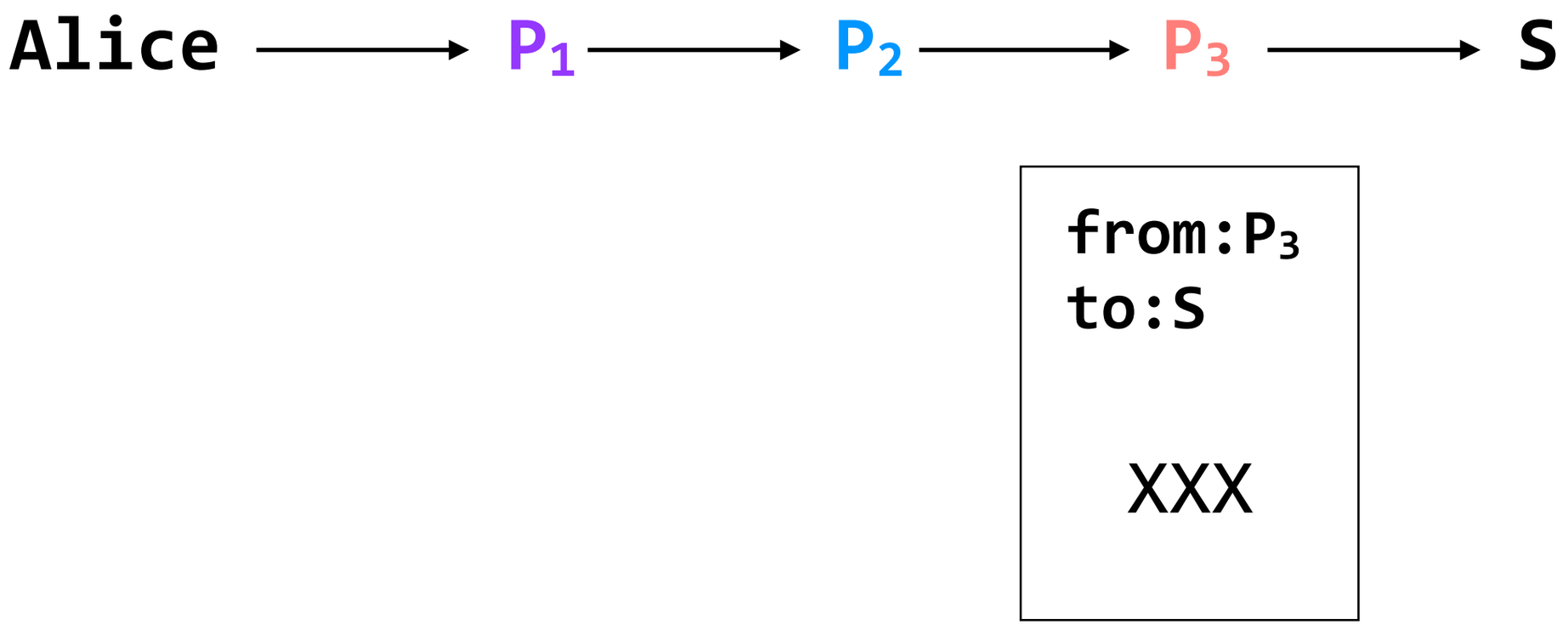
2. P_1 strips off one layer of encryption and edits the header



3. P_2 strips off one layer of encryption and edits the header

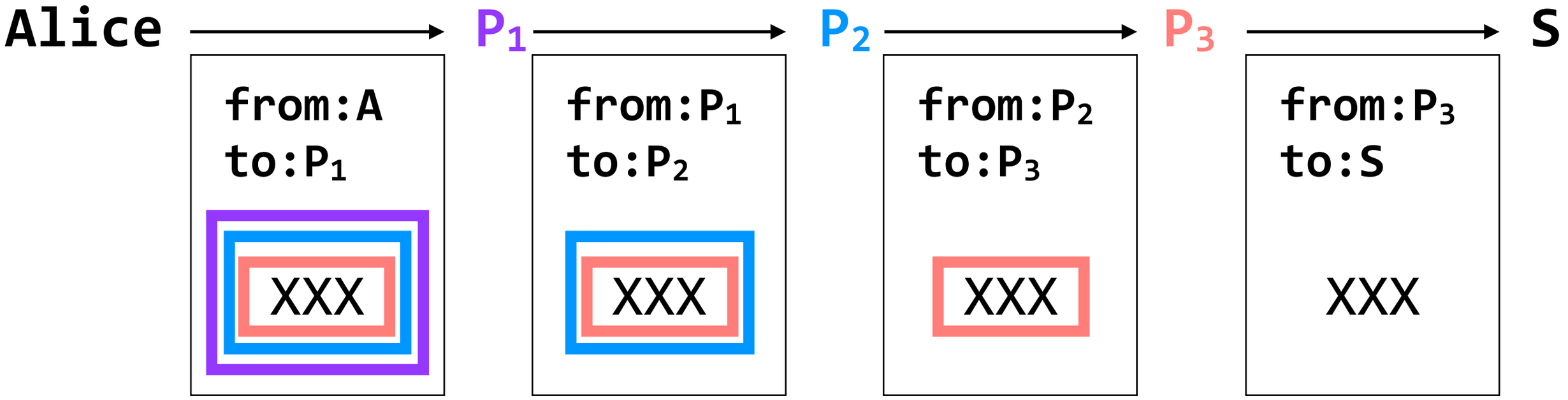


4. P_3 strips off one layer of encryption and edits the header



5. P_3 sends the packet to S

Katrina LaCurts | lacurts@mit | 6.033 2015



things to avoid

- 👍 no packet should say “from: Alice, to: S”
- 👍 no entity in the network should receive a packet from Alice and send it directly to S
- 👍 no entity in the network should keep state that links Alice to S
- 👍 data should not appear the same across multiple packets

digital currency

Katrina LaCurts | lacurts@mit | 6.033 2015

decentralized currency

can we avoid having a centralized bank?

technical challenges

- keeping track of who owns which coins
- assigning new serial numbers
- **verifying that a particular coin hasn't already been spent**

- **Tor** provides anonymity for users, preventing attackers from linking a sender to its receiver.

- **Bitcoin** is a decentralized digital currency. Being decentralized means that there is no bank; in Bitcoin, everyone is the bank.

- Both of these technologies deal, at least somewhat, with **anonymity**. But more importantly, they solve interesting technical problems and use cryptography (and other techniques) in clever ways. Understanding how they work and why they're used will give you a better sense of how secure you are online.