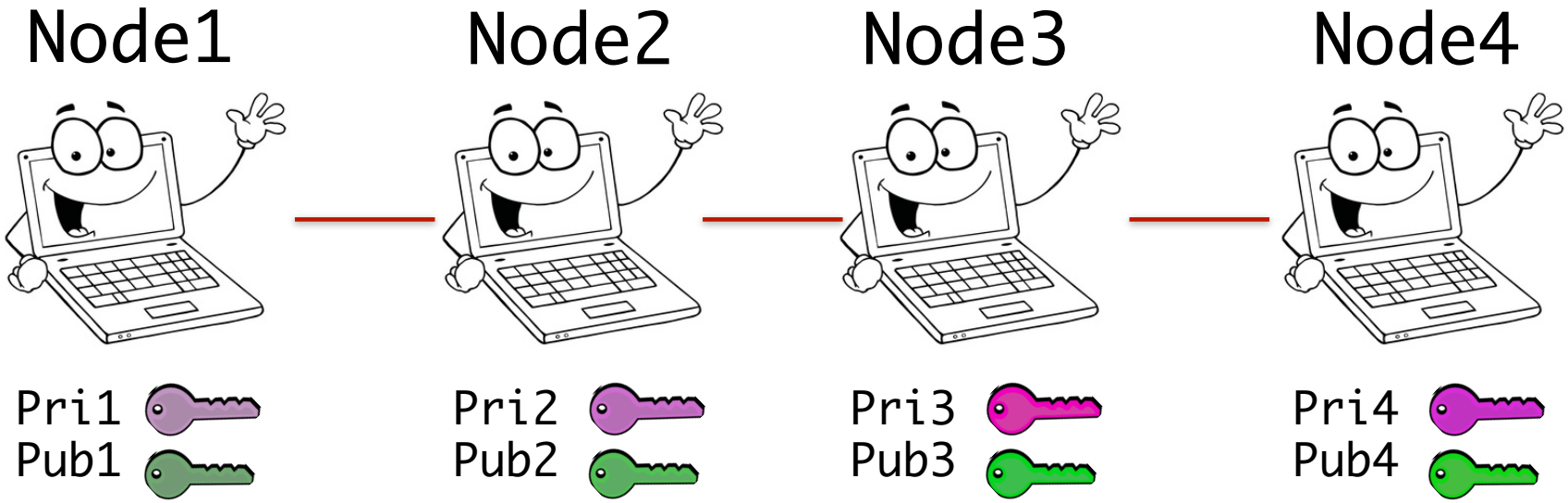
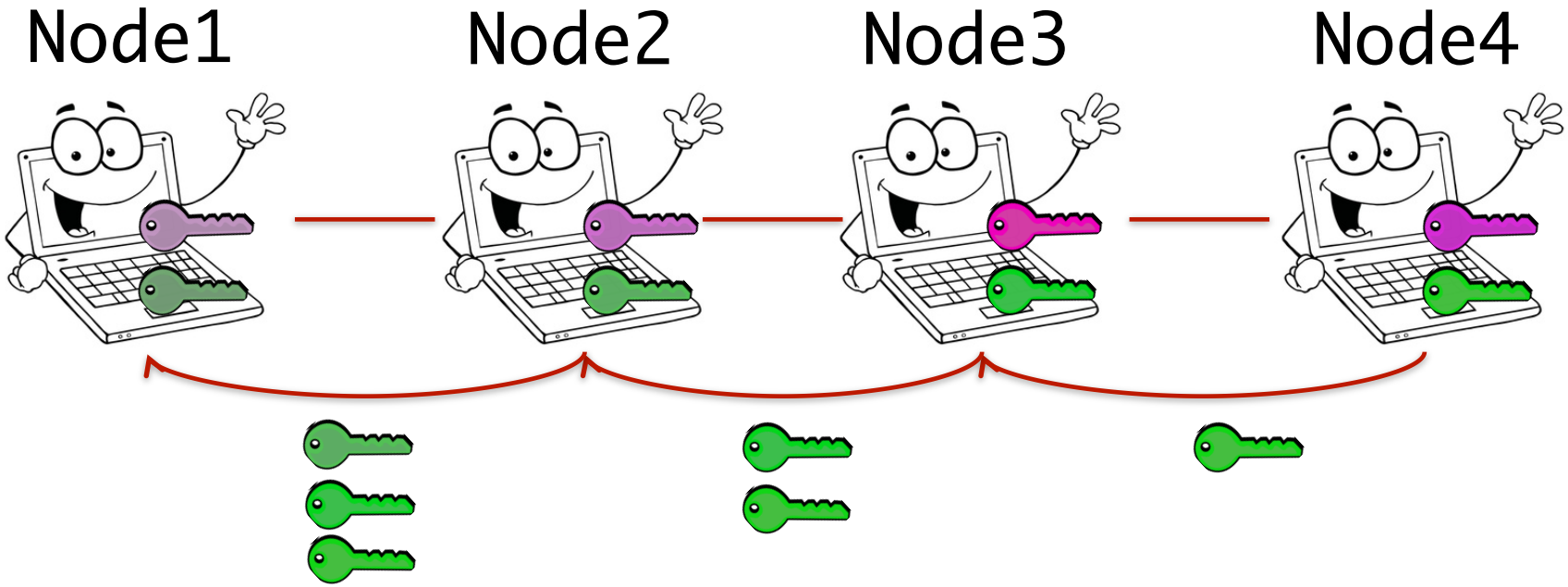
Onion Routing in Peerster

Tian Pan

Building Decentralized Systems Demo Session

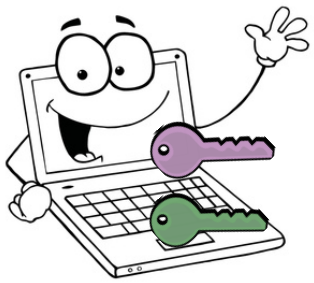


1. Each peerster generates a public-private key pair with RSA



2. Each peerster attaches its public key and NodeID to routing messages

Node1

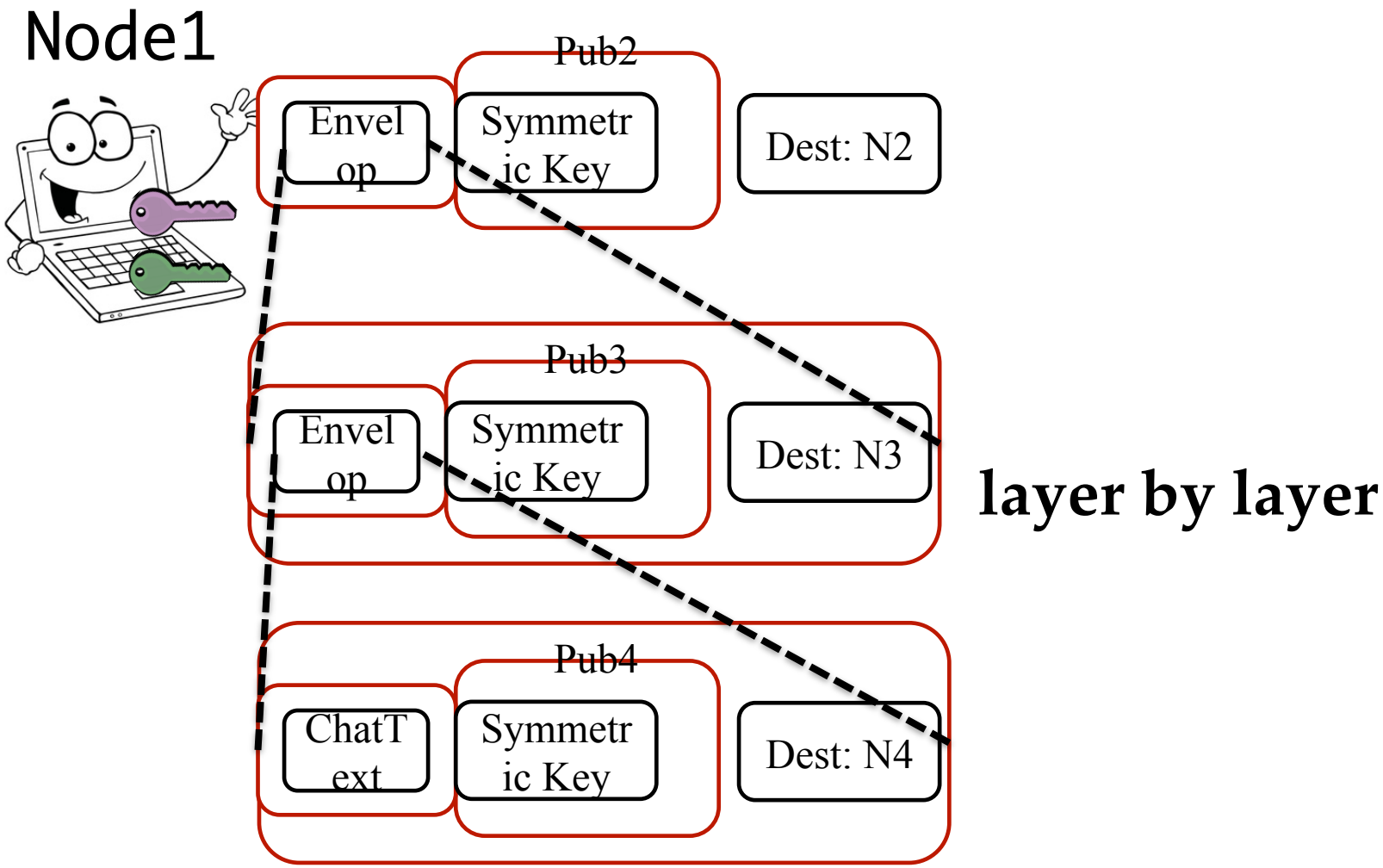


Next Hop Table	
N2	N2
N3	N2
N4	N2

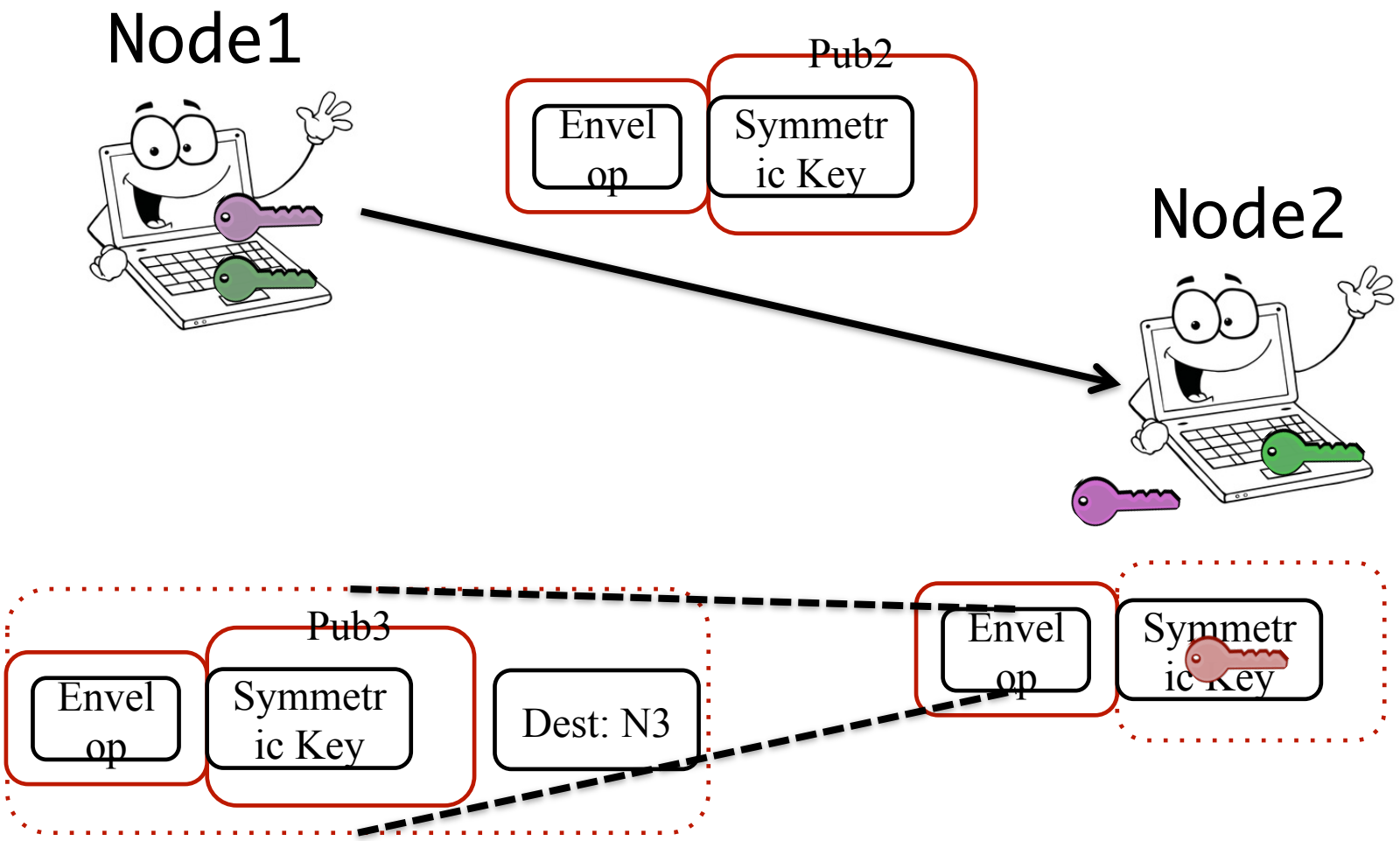
Path	
N2	N2
N3	N2 | N3
N4	N2 | N3 | N4

Keys	
N2	Pub2
N3	Pub2| Pub3
N4	Pub2| Pub3| Pub4

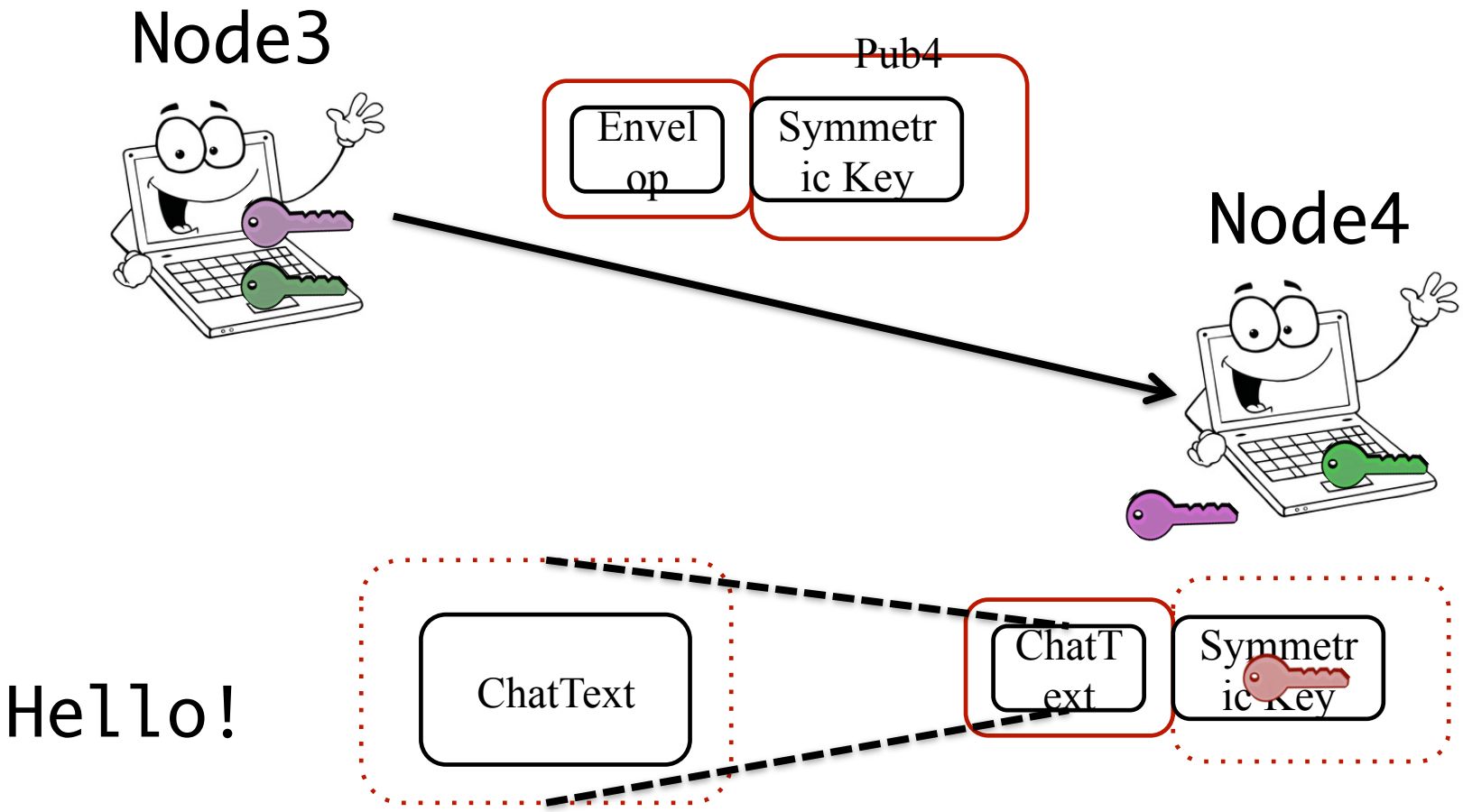
3. Each peerster maintains keys and path tables along with next hop table.



4. Encrypt the envelop with symmetric encryption (AES) for efficiency and encrypt the symmetric key with corresponding public key



5. Each node in the path decrypts the symmetric key with its private key, decrypts the envelop with symmetric key, and sends the inner envelop



6. … until there is only a "ChatText" in the envelop

It does not encrypt the envelop with RSA directly but uses an intermediate AES encryption, because

- Symmetric encryption is more efficient when encrypting big strings.
- RSA is not so secure for encrypting large texts.
- RSA can only encrypt data within a certain length and its result also has a certain length, which are all determined by the key length.

Initialization Vector (IV) can be sent in plain text.

Demo…

Thank you ~