Move Things From One Computer to Another, Safely

magic-wormhole.io

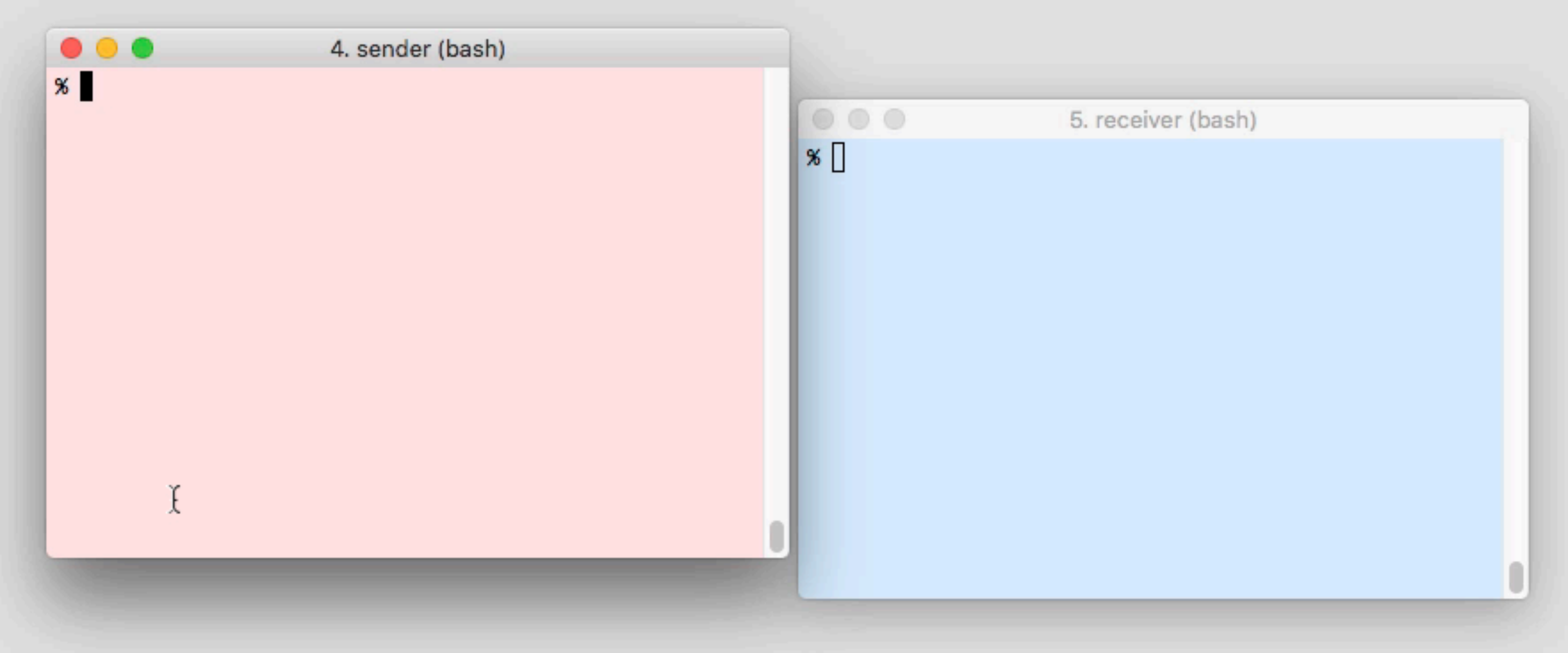
Brian Warner
@lotharrr

PyCon 2016
#magicwormhole

File (or directory or string) Transfer Program

- Securely moves a file from one computer to another
- Claim: easier than all other secure tools
  - Especially for moving to an unrelated computer

What It Looks Like

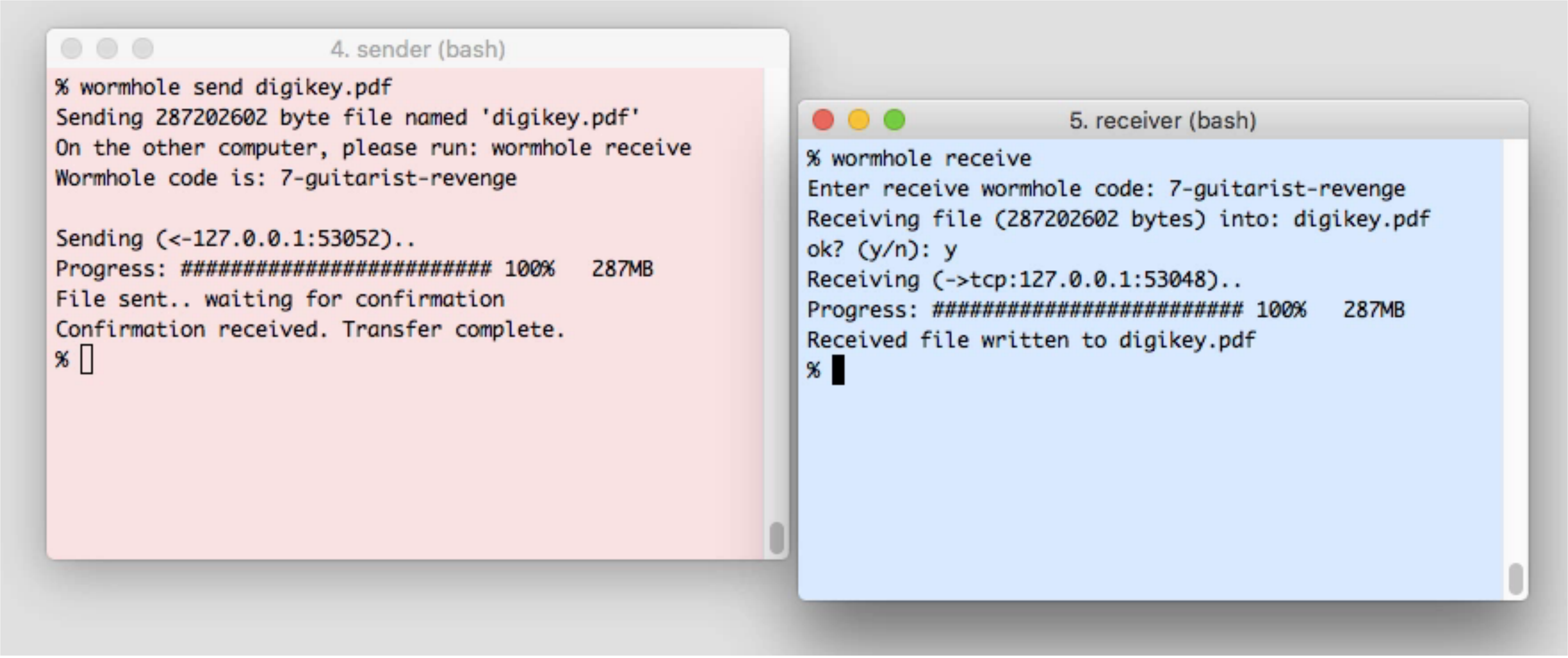


```
%
```

```
%
```

```
pip install magic-wormhole
```

What It Looks Like

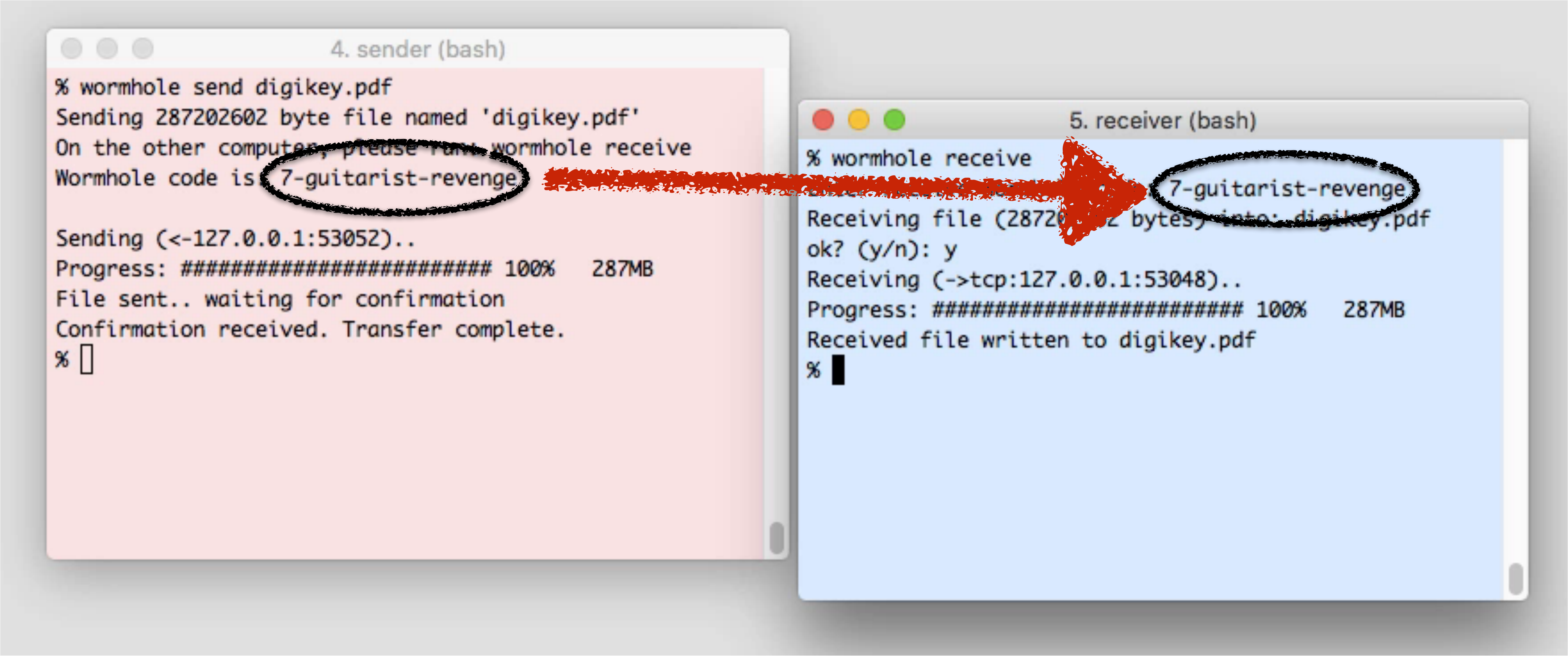


```
% wormhole send digikey.pdf
Sending 287202602 byte file named 'digikey.pdf'
On the other computer, please run: wormhole receive
Wormhole code is: 7-guitarist-revenge

Sending (<-127.0.0.1:53052)..
Progress: ######################### 100%   287MB
File sent.. waiting for confirmation
Confirmation received. Transfer complete.
%
```

```
% wormhole receive
Enter receive wormhole code: 7-guitarist-revenge
Receiving file (287202602 bytes) into: digikey.pdf
ok? (y/n): y
Receiving (->tcp:127.0.0.1:53048)..
Progress: ######################### 100%   287MB
Received file written to digikey.pdf
%
```

`pip install magic-wormhole`

What It Looks Like

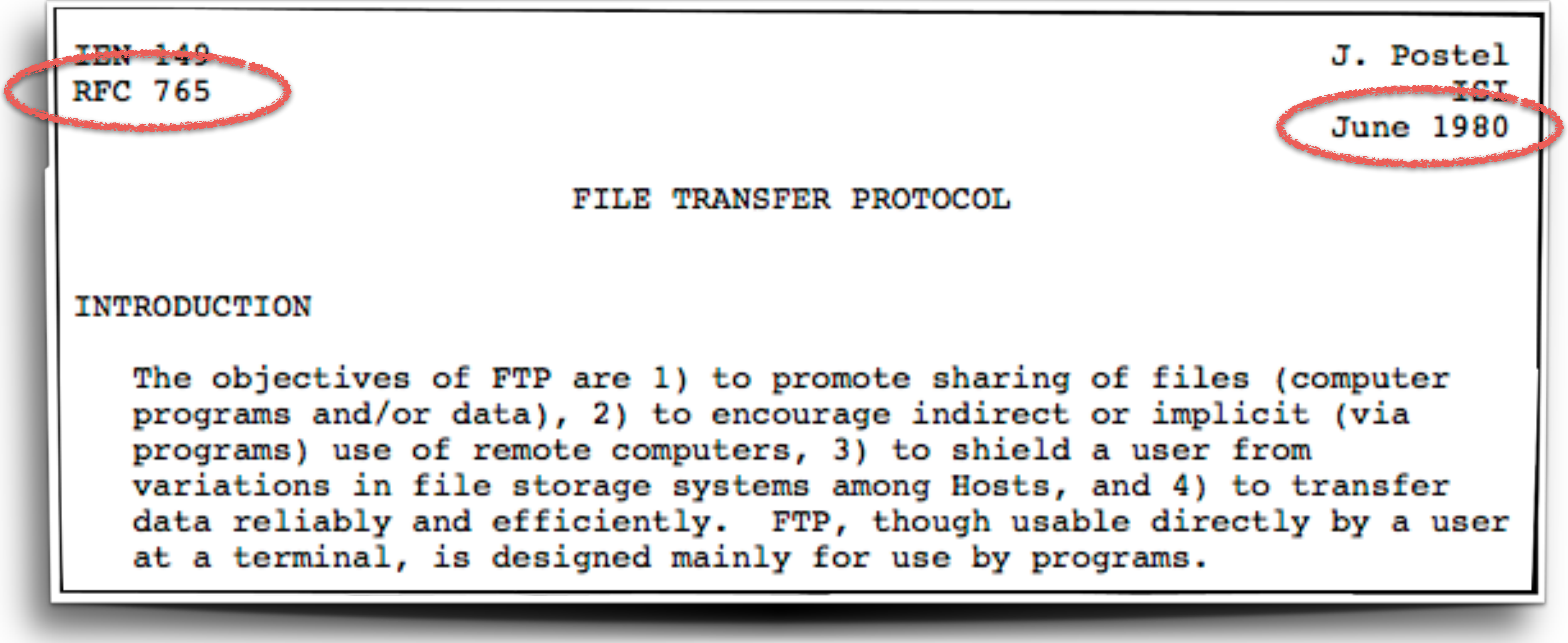


```
% wormhole send digikey.pdf
Sending 287202602 byte file named 'digikey.pdf'
On the other computer, please run: wormhole receive
Wormhole code is: 7-guitarist-revenge

Sending (<-127.0.0.1:53052)..
Progress: ######################### 100%   287MB
File sent.. waiting for confirmation
Confirmation received. Transfer complete.
% 
```

```
% wormhole receive
Enter receive wormhole code: 7-guitarist-revenge
Receiving file (287202602 bytes) into: digikey.pdf
ok? (y/n): y
Receiving (->tcp:127.0.0.1:53048)..
Progress: ######################### 100%   287MB
Received file written to digikey.pdf
% 
```

`pip install magic-wormhole`

Solved Problem?



```
IEN 149                                                    J. Postel
RFC 765                                                          ISI
                                                           June 1980

                          FILE TRANSFER PROTOCOL


INTRODUCTION

   The objectives of FTP are 1) to promote sharing of files (computer
   programs and/or data), 2) to encourage indirect or implicit (via
   programs) use of remote computers, 3) to shield a user from
   variations in file storage systems among Hosts, and 4) to transfer
   data reliably and efficiently.  FTP, though usable directly by a user
   at a terminal, is designed mainly for use by programs.
```

- What's wrong with the tools we currently use?

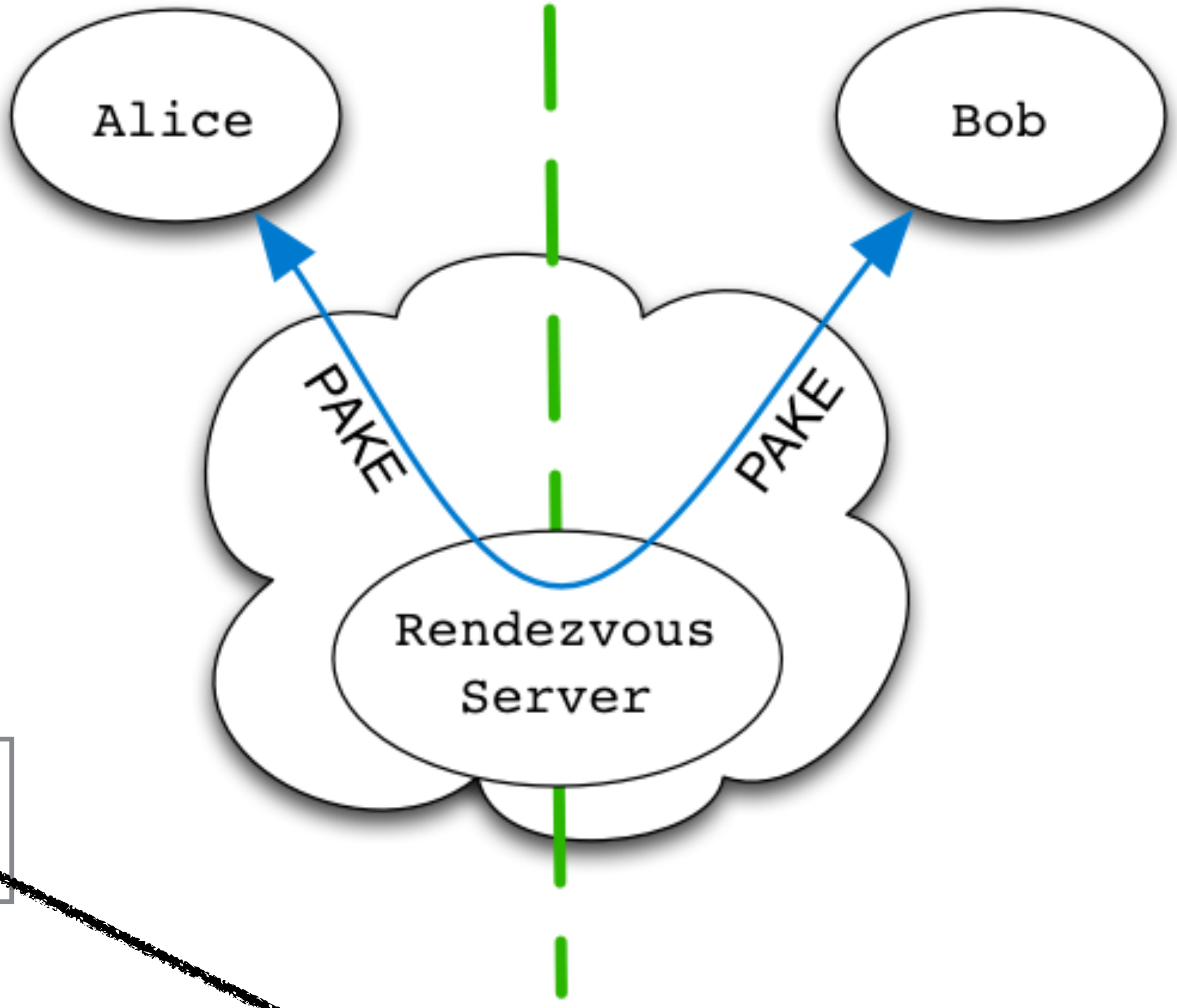
"easily". "safely".

	dictate string to sender	dictate string to receiver	needs proximity	eavesdroppers
send email	~30 chars			ISPs, CAs, internet
upload to FTP/HTTP		~60 chars		server, ISPs, CAs, internet
dropbox		~60 chars		Dropbox, CAs
+ URL shortener		~20 chars		Shortening Service, lucky guessers, Dropbox, CAs
USB drive			X	eww cooties
SSH/scp		~740 char pubkey		none
magic wormhole		**~20 chars**		**none**

How Does It Work?

- Rendezvous Message Exchange
- PAKE, Key Agreement
- IP Address Exchange
- Transit Connection
- Data Transfer

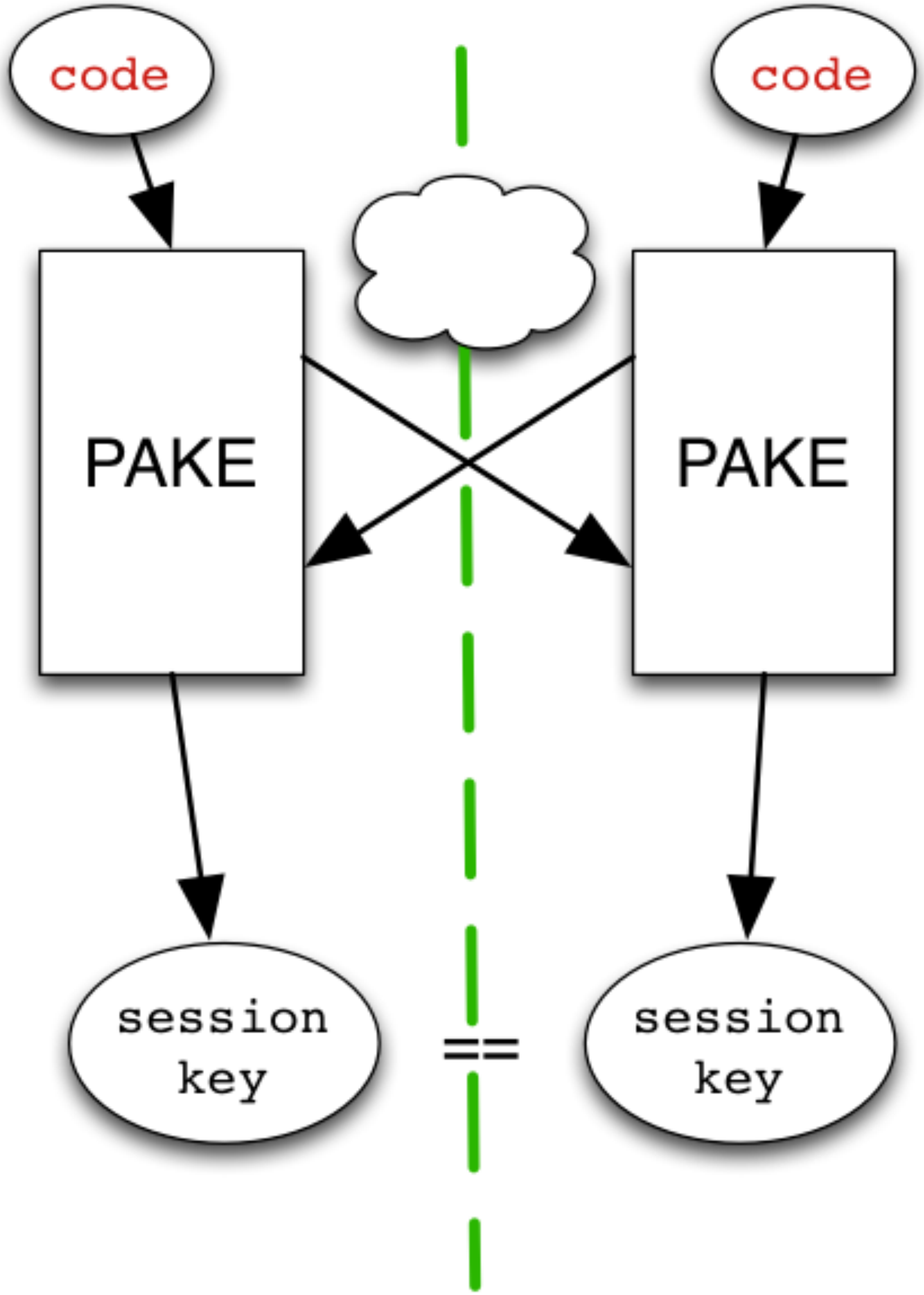
Rendezvous Server



Channel ID

typical code: `1-liberty-assume`

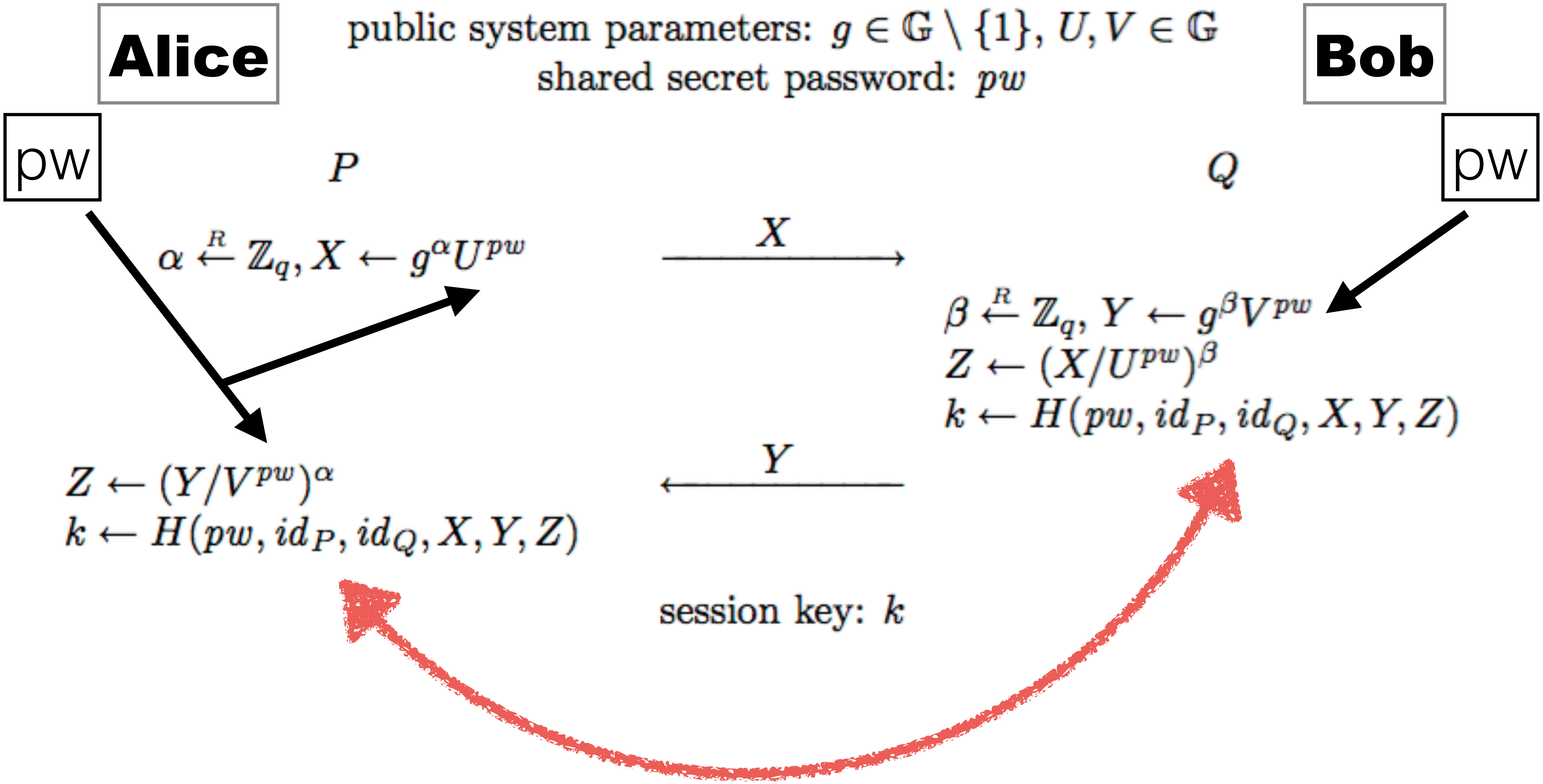
PAKE-based Security



P assword
A uthenticated
K ey
E xchange

1992: EKE
1997: SRP
2005: SPAKE2

SPAKE2



Alice

public system parameters: $g \in \mathbb{G} \setminus \{1\}, U, V \in \mathbb{G}$

shared secret password: pw

Bob

pw

P

Q

pw

$\alpha \overset{R}{\leftarrow} \mathbb{Z}_q, X \leftarrow g^{\alpha} U^{pw}$

$\xrightarrow{\quad X \quad}$

$\beta \overset{R}{\leftarrow} \mathbb{Z}_q, Y \leftarrow g^{\beta} V^{pw}$

$Z \leftarrow (X/U^{pw})^{\beta}$

$k \leftarrow H(pw, id_P, id_Q, X, Y, Z)$

$\xleftarrow{\quad Y \quad}$

$Z \leftarrow (Y/V^{pw})^{\alpha}$

$k \leftarrow H(pw, id_P, id_Q, X, Y, Z)$

session key: k

```
pip install python-spake2
```

diagram credit: Dan Boneh

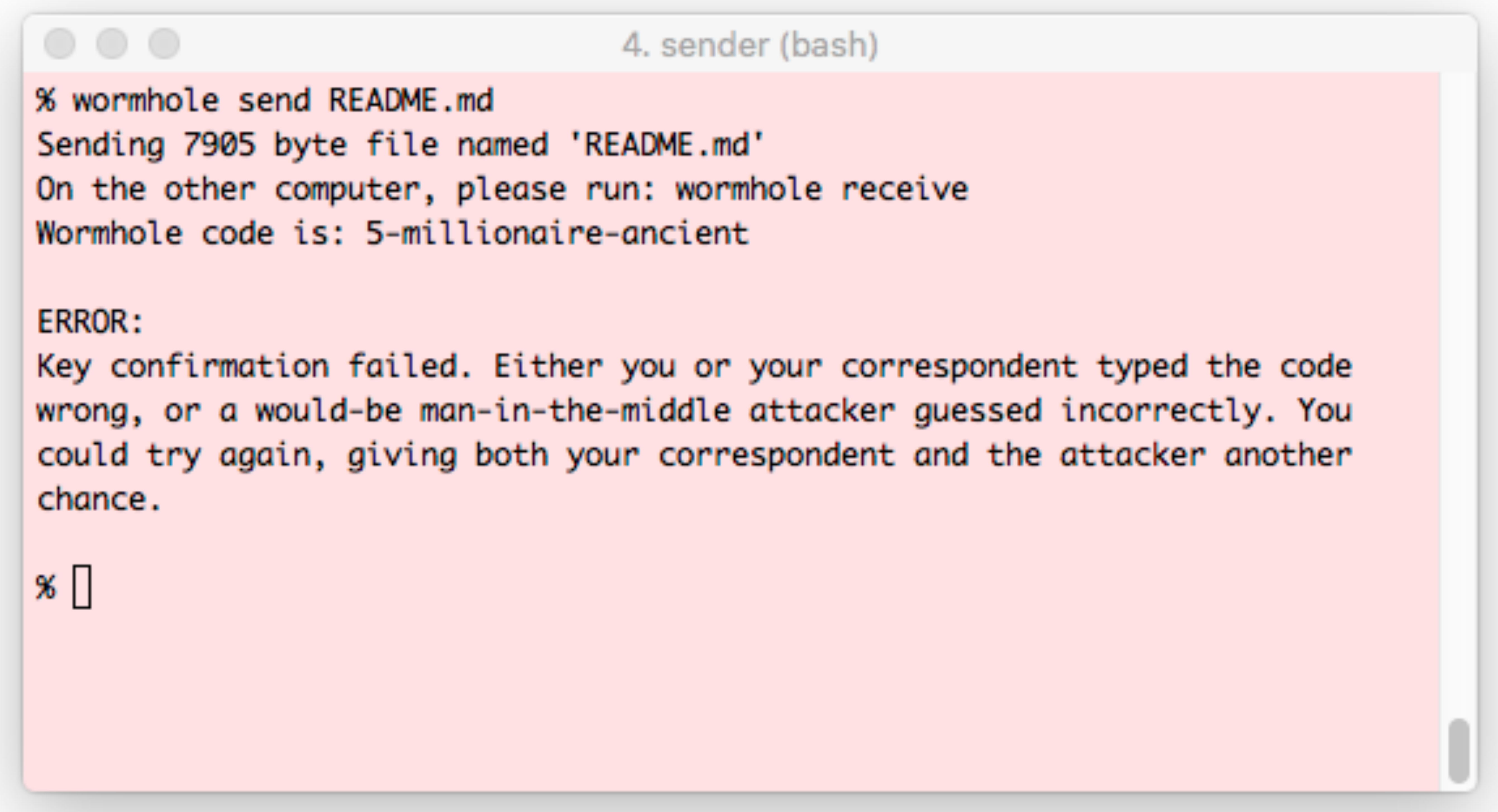
Security of PAKE

- Weak Secret + Interaction == Strong Secret
- Passive eavesdropper gets zero information
- Active MitM gets one guess per protocol run
  - failed guess == zero information
  - failed guesses are visible to users

Security of PAKE

- Wormhole codes are single-use, forward-secure
- Default code is 2 words (256-word list) == 16 bits
- User must retry 655 times before attacker has 1% chance of success

Laziness Improves Security

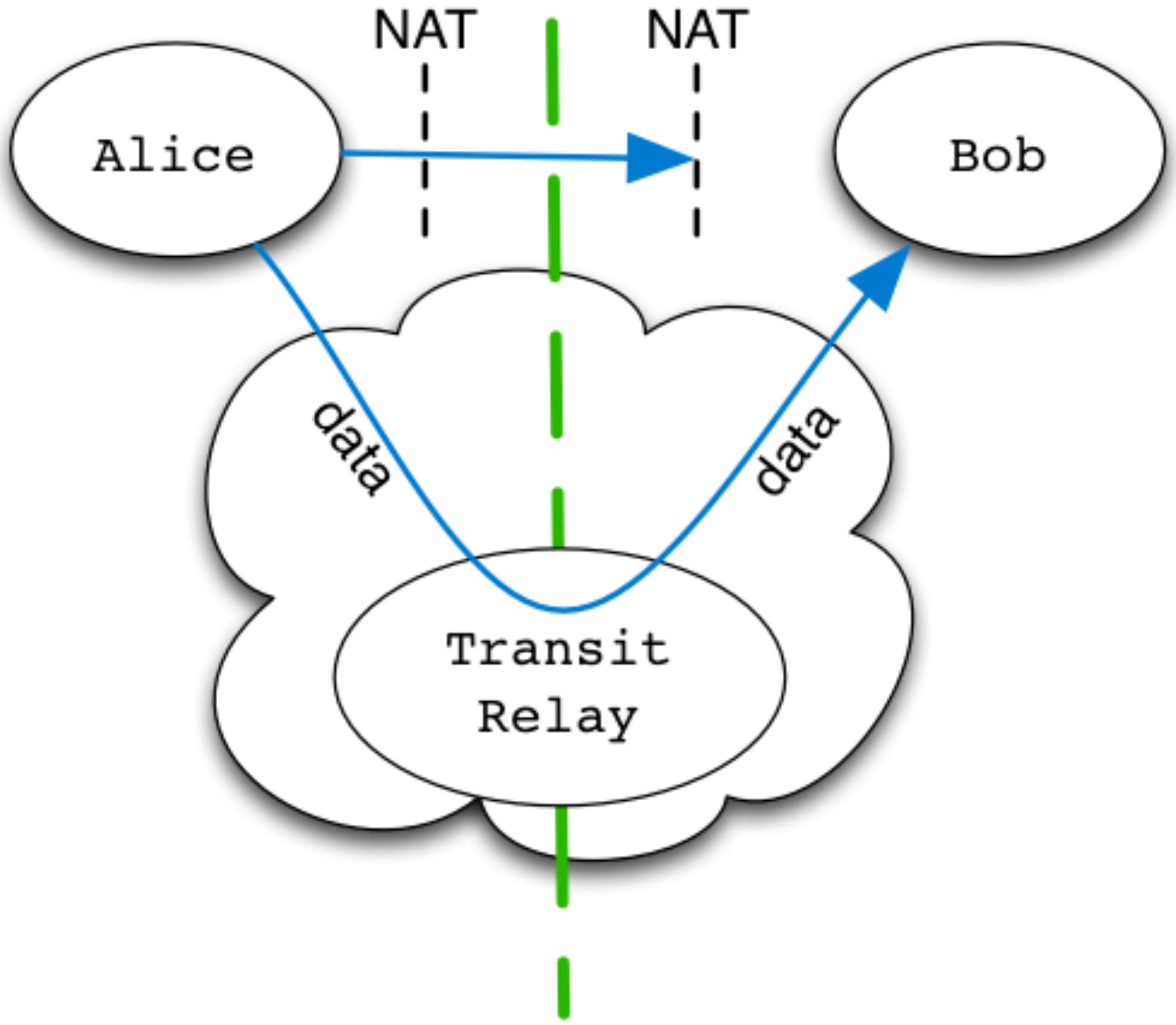


```
% wormhole send README.md
Sending 7905 byte file named 'README.md'
On the other computer, please run: wormhole receive
Wormhole code is: 5-millionaire-ancient

ERROR:
Key confirmation failed. Either you or your correspondent typed the code
wrong, or a would-be man-in-the-middle attacker guessed incorrectly. You
could try again, giving both your correspondent and the attacker another
chance.

% 
```

IP Address Exchange

- Find addresses with `ifconfig`
- Listen on TCP ports
- Exchange addresses+ports
- Try to connect, trade encrypted handshakes
- First successful connection wins

Data Relay Server



Encrypted Transit

- Provides encrypted record pipe
- Uses NaCl `SecretBox` (Salsa20/Poly1305)
- Keys are **`HKDF(masterkey, purpose)`**
- Data is hashed (SHA256) during transit
- Final ACK confirms the hash

Library API

```
w = wormhole(AppID, relay_url)

w.set_code("1-peachy-seabird")

w.send(b"hello")

answer = w.get()
```

Future Work

- GUI, pre-packaged installers, browser extension
- Negotiate better transports:
  - WebRTC, ICE/STUN, libutp
  - Tor Onion Services
- Add SPAKE2 to libsodium
- Port to other languages: JavaScript, Go, Rust

Beyond File Transfer

- Use this anywhere you need to deliver a credential
  - Provisioning new client devices
  - Pairing client devices to each other
  - Populating addressbook entries in communication/messaging systems

Provisioning Clients

Old	New
Type password into server	Get Wormhole code from server
Type password into client	Type code into client

Messaging Apps

Old	New
Alice sends public key to server	Alice shows Wormhole code to Bob
Bob asks server for Alice's key	Bob gets Alice's key from Alice (via wormhole)

Add PAKE to your Toolbox

- Cryptographic tools disseminate too slowly
- We need good examples, compelling use cases, helpful libraries
- File transfer is a foot in the door. PAKE is the rest.

Magic-Wormhole

Move Things From One Computer to Another,
Safely

magic-wormhole.io

https://github.com/warner/magic-wormhole

Brian Warner

warner@lothar.com

@lotharrr

Thanks To: Rackspace, Twisted, Glyph, djb, $2^{255}-19$