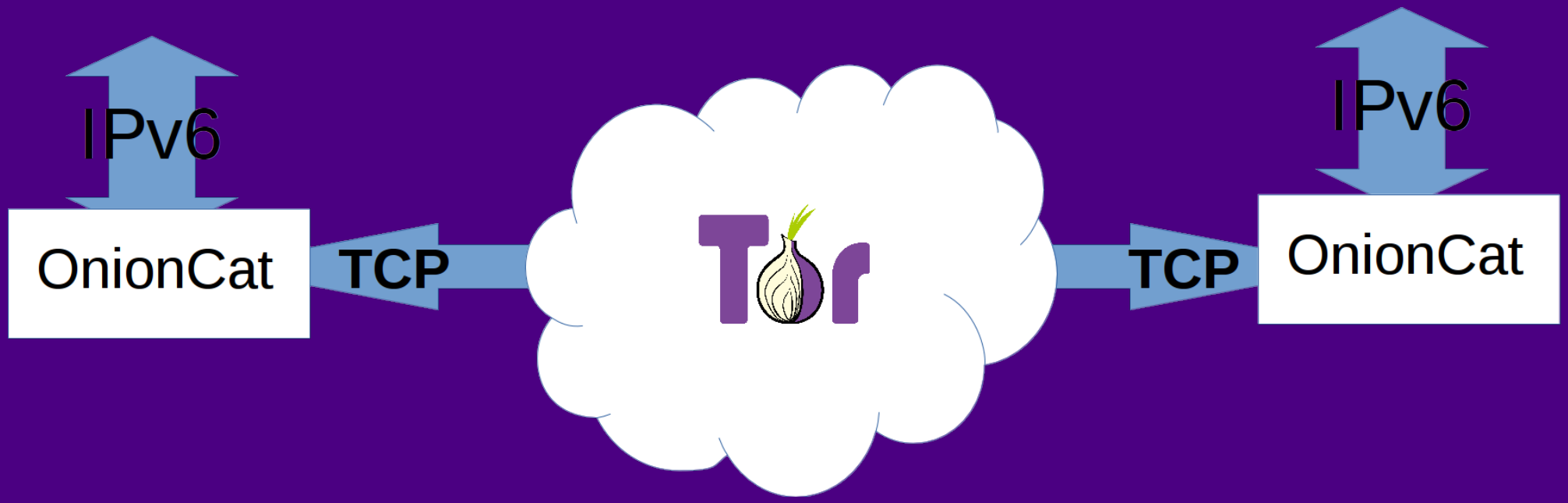
OnionCat and Tor's new Cryptosystem

Bernhard R. Fischer

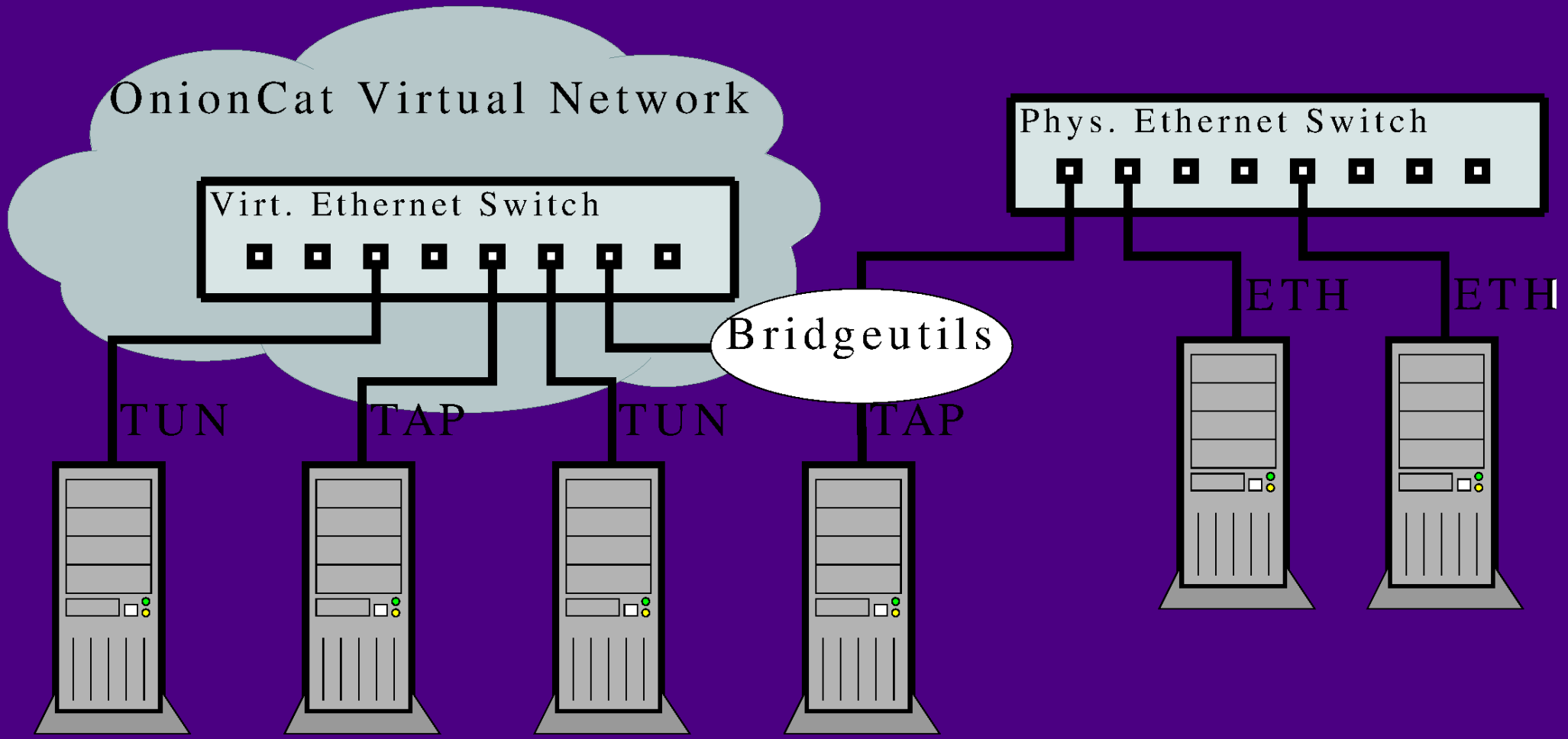
2048R/5C5FFD47, bf@abenteuerland.at

ITSecX 2014

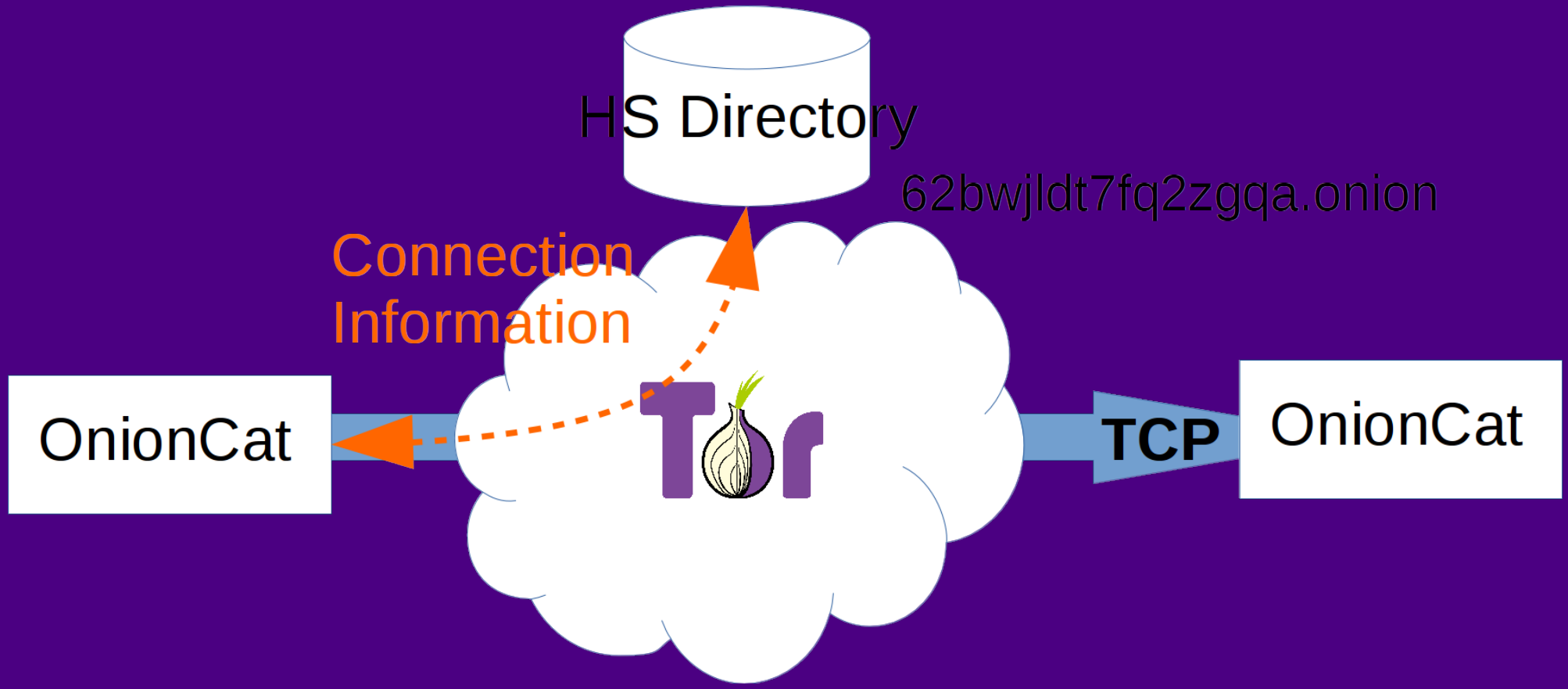
OnionCat Overview



OnionCat User Perspective



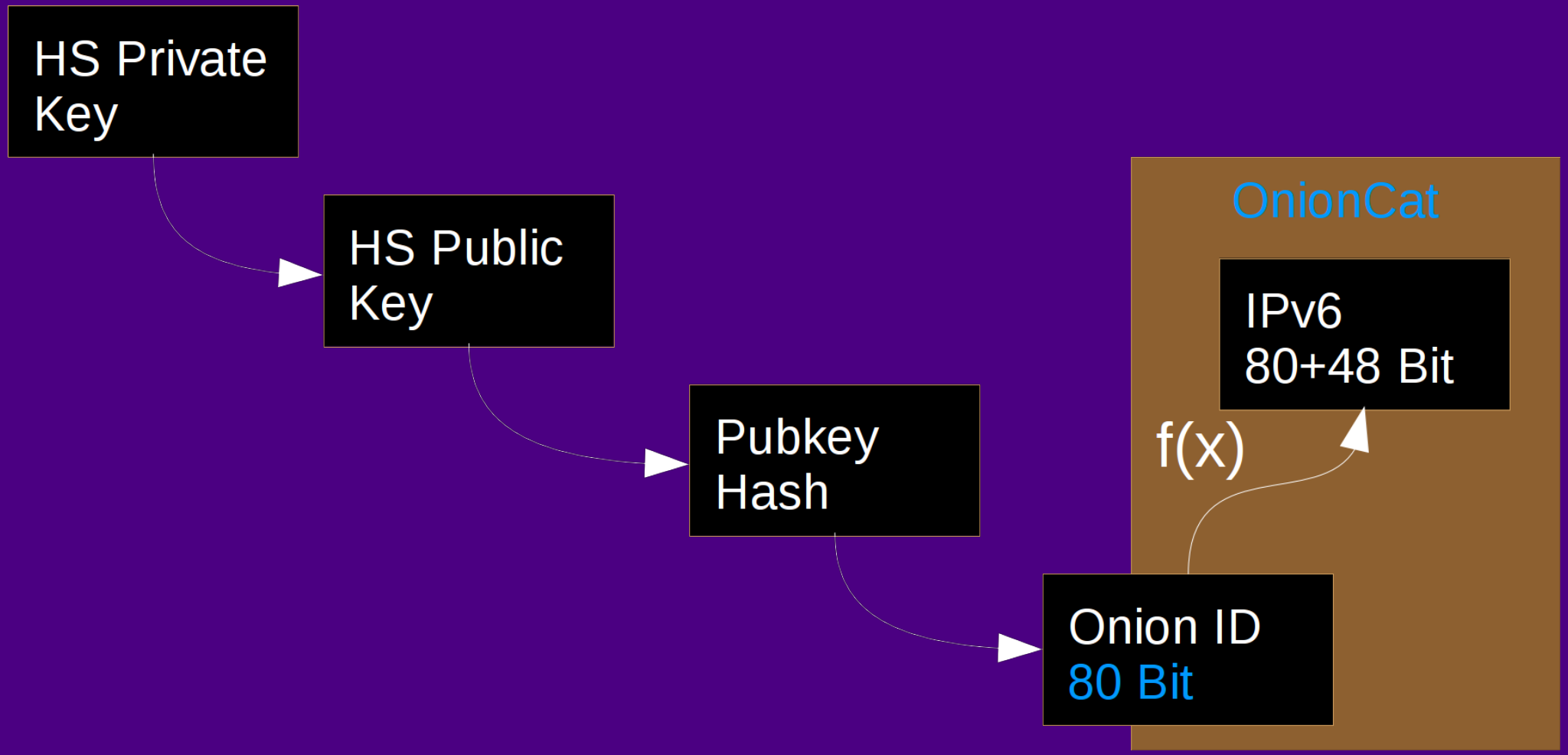
OC, Tor, and HIDDEN Services



HS Directory

- Is a database
- Contains the hidden service descriptors
- Primary key: Onion-ID (62bwjldt7fq2zgqa.onion)
- + (Connection) Information
- + Digital signature

The Onion ID


HS Private Key
HS Public Key
Pubkey Hash
Onion ID
80 Bit
f(x)
OnionCat
IPv6
80+48 Bit

OC Connection Setup

- OC receives IPv6 packet
- Converts destination IPv6 (of packet) back to Onion ID

  OnionID = f'(IPv6) = IPv6:80
- Requests Tor HS circuit
- Forwards IPv6 packets back and forth

Conversion IPv6/OnionID

- IPv6 = f(OnionID) ... simply add IPv6 prefix fd87:d87e:eb43::/48
- OnionID = f'(IPv6) ... strip prefix.

Tor's New Cryptosystem

Increased bit length of Onion IDs...

128, 256, 512,...?

IPv6 = f(OnionID) ... this is easy :)

OnionID = f'(IPv6) ... ?

HOW DO WE GET THE LOST BITS BACK?

Getting the lost bits back

There is no algorithm to generate knowledge without anything.

The solution is a database.

E.g. DNS, or any new DB infrastracture (M. Fic, DHT).

JUST TROUBLES, TROUBLES, TROUBLES...

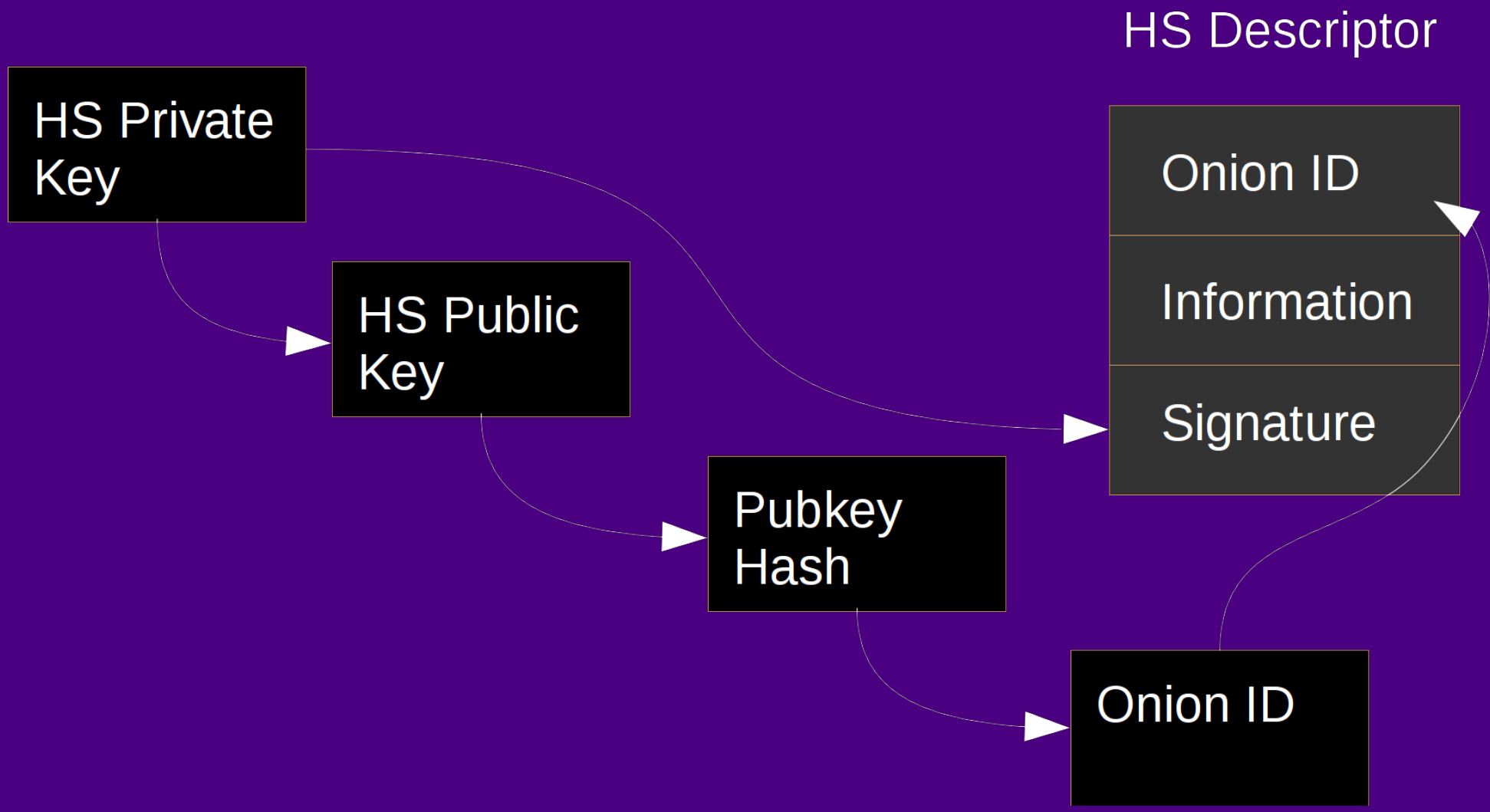
Using the HS Directory

Add a helper entry to the HS directory.

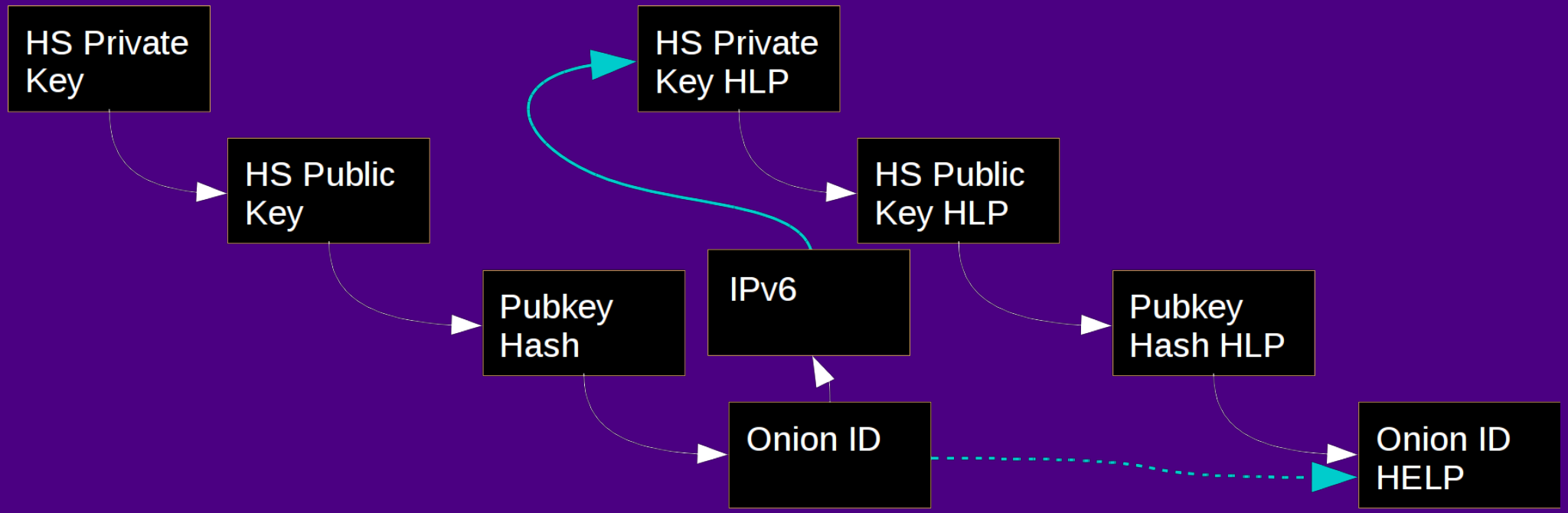
- Convert and append a defined value to the IPv6 address.
- E.g. abababababababab62bwjldt7fq2zgqa.onion.
- Store real ID into the information field of the HS descriptor.
- Every OC publishes its helper entry.
- On outgoing connections, OC looks up the information in those helper entries.

Does this work?

How to create a valid signature?



We need a PRIVATE KEY



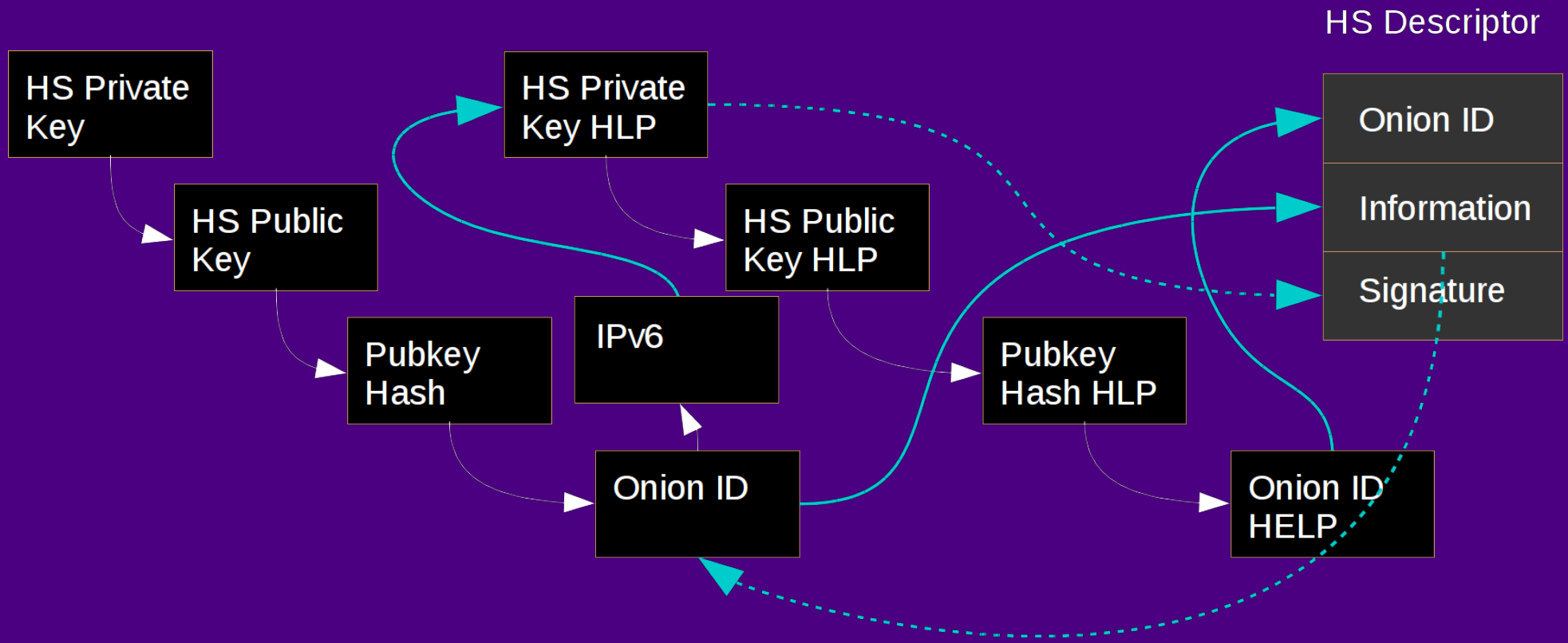
Deterministically create an RSA key

RSA private key: 2 prime numbers p, q, 2 exponents d, e

Find the next 2 prime numbers of the OnionID!

Needs a few milliseconds on my Laptop :)

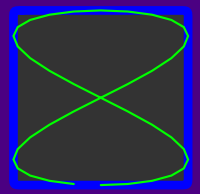
The Big Picture



Weaknesses

Yes, there is the possibility of a DOS.

The HS descriptor can easily be overwritten.



QUESTIONS?