Changes in this version
context = concat(mode, ciphersuite, enc, pkRm, pkIm, len(pskID), pskID, len(info), info)

secret = Extract(psk, zz)
key = Expand(secret, concat("hpke key", context), Nk)
nonce = Expand(secret, concat("hpke nonce", context), Nn)
Running Code

Go implementation by Richard Barnes

- All ciphersuites **plus SIKE** (thanks Nick!)  
  +154 -22

  ![GitHub](https://github.com/bifurcation/hpke)

Python implementation by Dave Cridland

- Follows document pseudocode very closely
- [https://github.com/dwd/crypto-examples/](https://github.com/dwd/crypto-examples/)

**TODO:** Interop, test vectors, verified implementation(s), ...
Limitations and Non-Goals

Forward Secrecy: **None**

- Meant as a primitive to be used in other protocols

Key Compromise Impersonation (KCI) Resistance: **None**

- Not possible with a “one round” KEM-based protocol

Post-Quantum Ciphersuites: **Not Right Now**

- Selections still ongoing
- Feasibility validated in code
Questions
Too Much?

Should we keep all four modes? (Base, PSK, Auth, PSKAuth)

Are folks OK with unified logic => optional / default inputs?
Combined
Asymmetric /
Symmetric
Hybrid
Encryption
Wrapping
Analysis

[[ Your name here ]]