circa 90 tests
around 800 test vectors
found at least 92 bugs in 10 implementations

improved implementations
improved our understanding of the ecosystem
highlights areas where implementations lack guidance
black box
  - consumer tests
  - producer-consumer tests
common interface
  - Stateless OpenPGP interface

$ sqop generate-key >key
$ sqop sign key <msg >sig
$ rpmsop verify sig key <msg
What’s next?

- test features from the crypto refresh while we refine it
  - most artifacts created by Sequoia
  - but can be shipped as files
- publish results with a focus on the crypto refresh
  - tag relevant tests
  - target development versions
- → well-understood and implementable spec
- → speed-up adoption
What can you do?

- standardization enthusiast
  - help curate a list of useful tests
  - write tests
  - review tests and results

- implementor
  - tell me how to get/build/update your (SOP) implementation
  - consider implementing your own SOP frontend
    - if you do, clue me how to keep it up-to-date
  - get in touch, be responsive
Join the Fun?

- add tests
  - talk to me
  - open an issue
- add an implementation
  - AWESOME!
  - implement the Stateless OpenPGP interface
  - talk to me
- argue semantics
  - talk to me
  - open an issue
  - discuss on openpgp@ietf.org

run the test suite

$ git clone https://gitlab.com/sequoia-pgp/openpgp-interoperability-test-suite
$ less README.md # optional; YOLO
$ apt install sqop # optional
$ cp config.json.dist config.json
$ editor config.json
$ cargo run --
  --retain-tests keyword
  --html-out results.html
  --json-out results.json