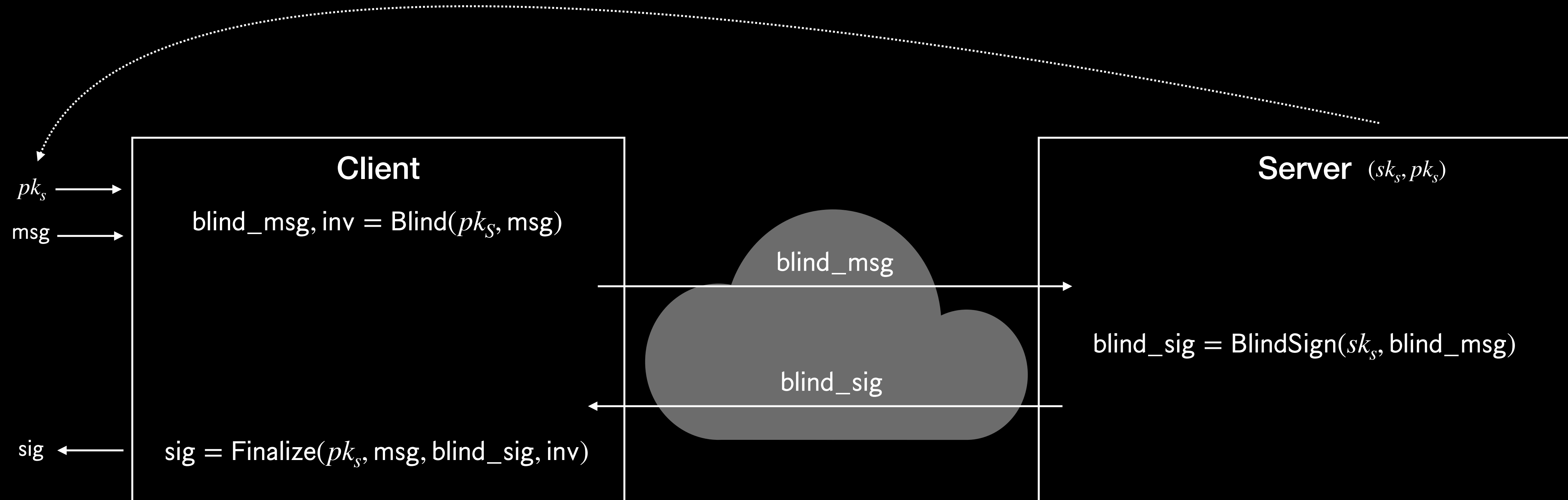


Blind RSA Signatures

`draft-irtf-cfrg-blind-rsa`

Denis, Jacobs, Wood - IETF 111 - CFRG

Blind RSA Protocol



Draft Status

Updates and implementations

Draft updates:

- Add deterministic signature recommendation, test vector, and API considerations
- Improve security consideration
- Editorial cleanup

More interoperable implementations added

Questions

Closing remaining issues

Open questions:

- Should we consider changing the name? [#1](#)
- Should the draft support partially blind signatures? [#29](#)
- Should the draft add other blind signature schemes? [#83](#)

Questions

Closing remaining issues

Open questions:

- Should we consider changing the name? [#1](#)
- Should the draft support partially blind signatures? [#29](#)
- Should the draft add other blind signature schemes? [#83](#)

Proposal: **close all issues as WONTFIX**

Ready for RGLC?