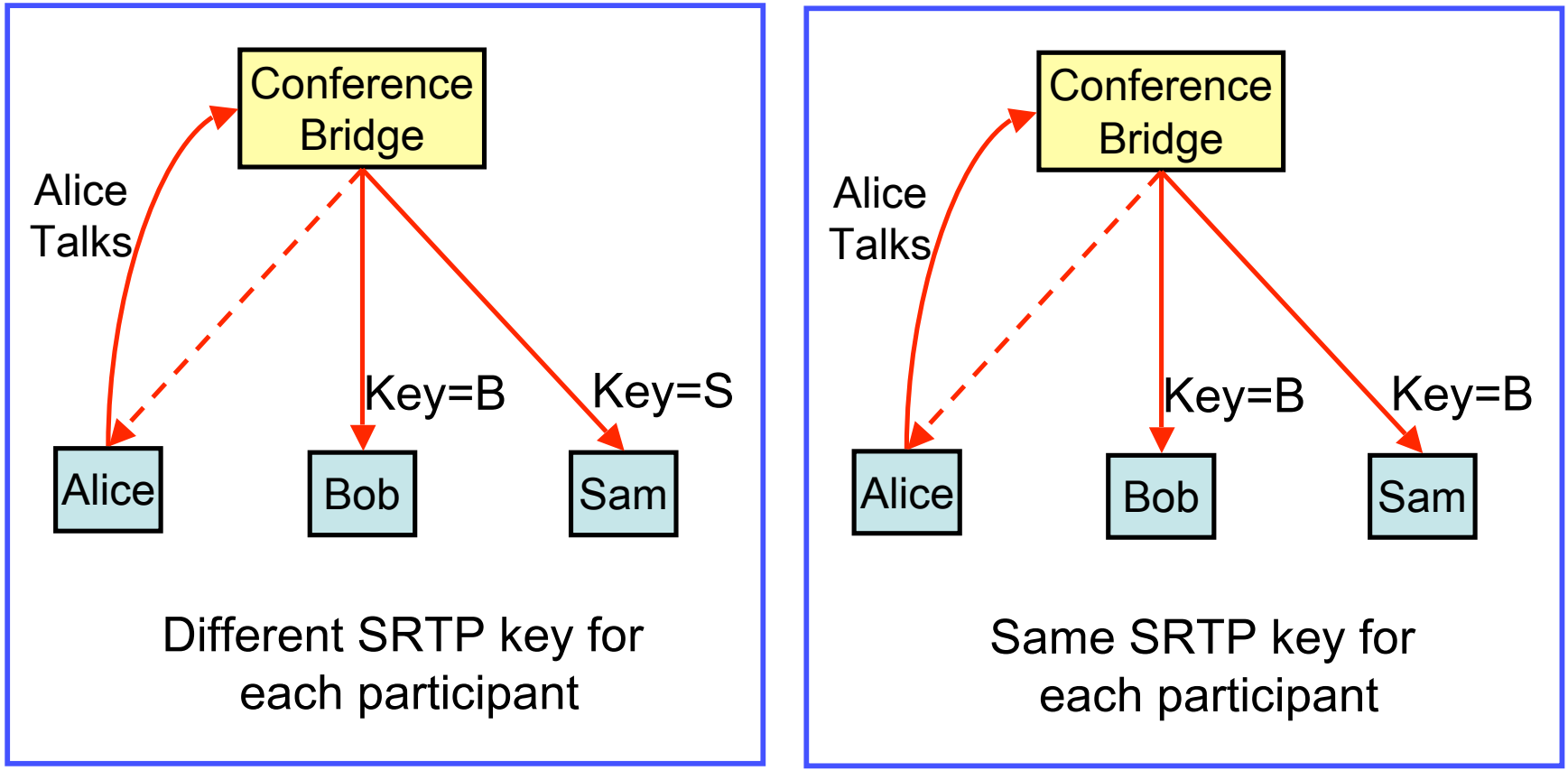
Shared-Key Conferencing Alternatives

David McGrew
Eric Rescorla

Conferencing/Push-to-Talk



Unique key conferencing

Shared-key conferencing

Issue: cost of encrypting for each stream

Unique Key Conferencing

- Bridge negotiates individual keys with each conference participant
  - Easy to support this mode already
- Security is easy
  - Source authentication between participants
  - Revocation of membership easy
- Bridge separately protects traffic to each receiver
  - Crypto cost ~ *N* (codec cost constant)

Shared Key Conferencing

- Bridge provides group key to each participant
  - Same key protects traffic to all receivers
- Performance easy
  - Crypto cost constant
- Security harder
  - Revocation requires re-establishment of group key
  - PFS would require ~ *N* work
  - No source authentication between participants
- SRTP coordination required
  - Can use EKT

Conferencing Options

- Requirements
  - Signaling support
  - Both dial-in and dial-out
  - Avoid race condition for key ‘ownership’
- Alternatives
  - Unique key
    - Performance concerns
  - Establish shared key in handshake
    - More complicated handshake
  - Re-key with shared key
    - Simpler but higher latency