Secure Multi-Track Computation

Jon Callas

Situation

- At a conference that has N tracks of talks

- You want to listen to more than one track

Possible Solutions

One

- Have a partner in the other session
- Use *multi-party computation* to construct composite talk with content of one in speaker pauses of the other
    - Can exceed information-theoretic limits of listener

Two

- Stand between tracks
- One way encryption to receive one or the other
- Drawbacks
  - You don't know which talk you're listening to
  - Listening position requires a *shortest vector* solution

Three

- Don't go to either talk
- Use *zero-knowledge* and *obfuscation* to convince people you did
- Drawback
    - You end up reading a lot of papers later

Four

- Consider the abstract to be a hash function of the paper
- Use *impossible differentials* in the *nonce* of the compression function as a *pre-image attack* on the full paper
  - (Search for terms in the ebook)
- This is *practical* and *efficient* if you're sober