

Big Fancy Title Here

Secure *Peer-to-Peer* system

Your truly
Someone else

Another slide title

1. Some text

Another slide title

1. Some text

- Some more text \mathbb{Z}

Another slide title

1. Some text

- Some more text \mathbb{Z}
- Semântica da aplicação: *"I'm Ed Snowden!"*
Leakage: stream correlation!!

Yet another title

1. Foo

Yet another title

1. Foo
2. Continue enum into next slide

Enough already!

3. Bah

Enough already!

3. Bah

Enough already!

3. Bah

State of the art

Block cipher security

- No “one size fits all” definition.
- Maximise resistance to (*known!*) attacks.
- Future-proof design: what about *unknown* attacks?
- Can simplicity be a prerequisite for security?

State of the art

Block cipher security

- No “one size fits all” definition.
- Maximise resistance to (*known!*) attacks.
- Future-proof design: what about *unknown* attacks?
- Can simplicity be a prerequisite for security?

State of the art

Block cipher security

- No “one size fits all” definition.
- Maximise resistance to (*known!*) attacks.
- Future-proof design: what about *unknown* attacks?
- Can simplicity be a prerequisite for security?

State of the art

Block cipher security

- No “one size fits all” definition.
- Maximise resistance to (*known!*) attacks.
- Future-proof design: what about *unknown* attacks?
- Can simplicity be a prerequisite for security?

Questions?

