Assumptions

Jon Callas
Yvo Desmedt

Our Core Assumptions

- Basic complexity theory
- Modern Physics describes the universe
- We can build machines that work

Complexity Assumptions

- We don’t know that factoring is hard
    - or discrete log, CDH, DDH, RSA, etc....
- It seems reasonable
- Even if it’s not hard, it might be hard enough

Physics Assumptions

- Quantum cryptography is built on **Physics**
  - Doesn't rely on unreliable complexity theory
- But
  - Side-channels can still exist
  - Assumes physics describes the universe

Physics Assumptions

- One-Time Pads
    - Assumes randomness exists
        - Einstein? Dice?
    - Assumes it can be extracted

Implementation Assumptions

- Is it possible to know if there are intentional flaws in hardware?
- Do we actually need intentional flaws to ruin a system?

Our Core Assumptions

- We believe in complexity theory
- We believe Physics describes the universe
- We believe we can build machines that work

Our Core Assumptions

- We believe in complexity theory
- We believe Physics describes the universe
- We believe we can build machines that work

Our Core Assumptions

- We **believe** in complexity theory
- We **believe** Physics describes the universe
- We **believe** we can build machines that work

Our Core Assumptions

- We believe in complexity theory
- We believe Physics describes the universe
- We believe we can build machines that work

Modern Cryptography

Modern Cryptography

=

Modern Cryptography

=

Faith-Based

Cryptography

Impact

- Can funding agencies fund religion?

Faith-Based Cryptography