Bridging the Gap Between Cutting Edge Cryptography and Practice

Challenge:

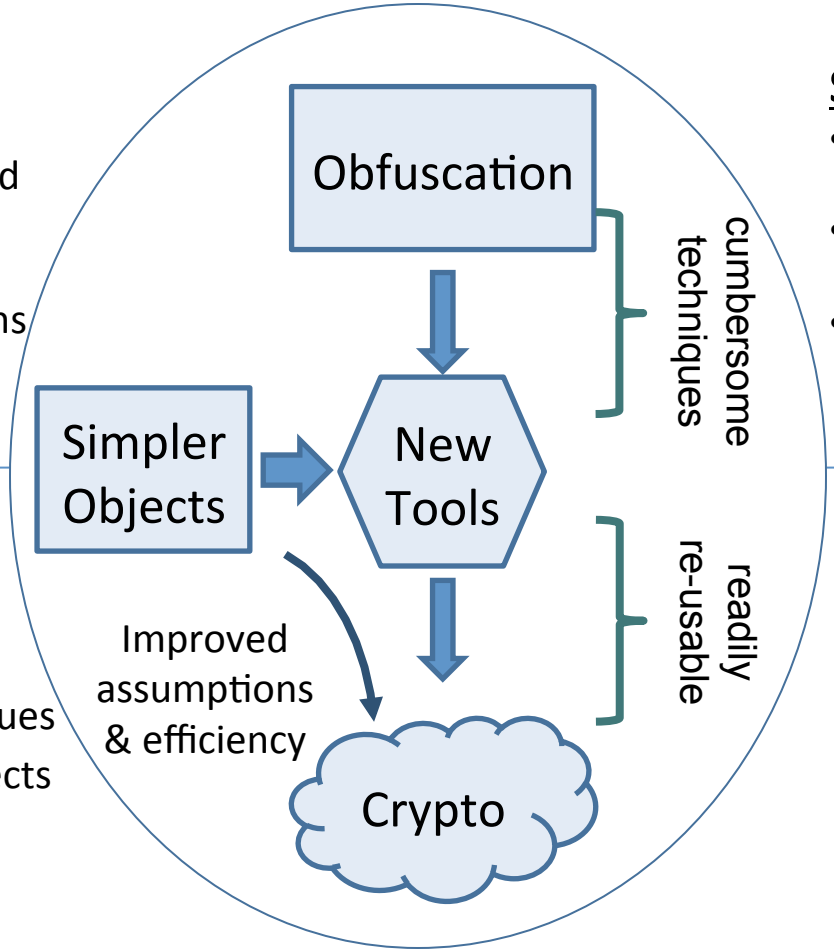
Cutting edge crypto based on obfuscation:

- Highly inefficient
- Untested assumptions
- Complicated techniques

Solution:

New cryptographic tools

- Abstract away complicated techniques
- Base on simpler objects than obfuscation



Scientific Impact:

- Easier to design new cryptosystems
- Unified approach to certain problems
- Improved efficiency, assumptions

Broader Impact:

- Toward a more secure cloud infrastructure
- Collaborative project
- Course on obfuscation, cryptography

Award 1616442
Princeton University
Mark Zhandry (mzhandry@princeton.edu)