# New Cryptography Libraries from Microsoft Research

Brian LaMacchia, Tolga Acar

Microsoft Research

Crypto Rump Session, 2014

# Two New Cryptography Libraries

- High performance ECC Library implementing new NUMS curves (C, intrinsics, assembler)
  - http://research.microsoft.com/projects/nums/
  - Full paper at http://eprint.iacr.org/2014/130
- JavaScript Cryptography Library
  - W3C WebCrypto API, polyfill ready
  - Big Integer arithmetic
  - Supports several browsers
  - http://research.microsoft.com/projects/msrjscrypto/
- Both libraries released under Apache 2.0
- Comments, questions, feedback, bug reports? Please send to msrsc@microsoft.com.