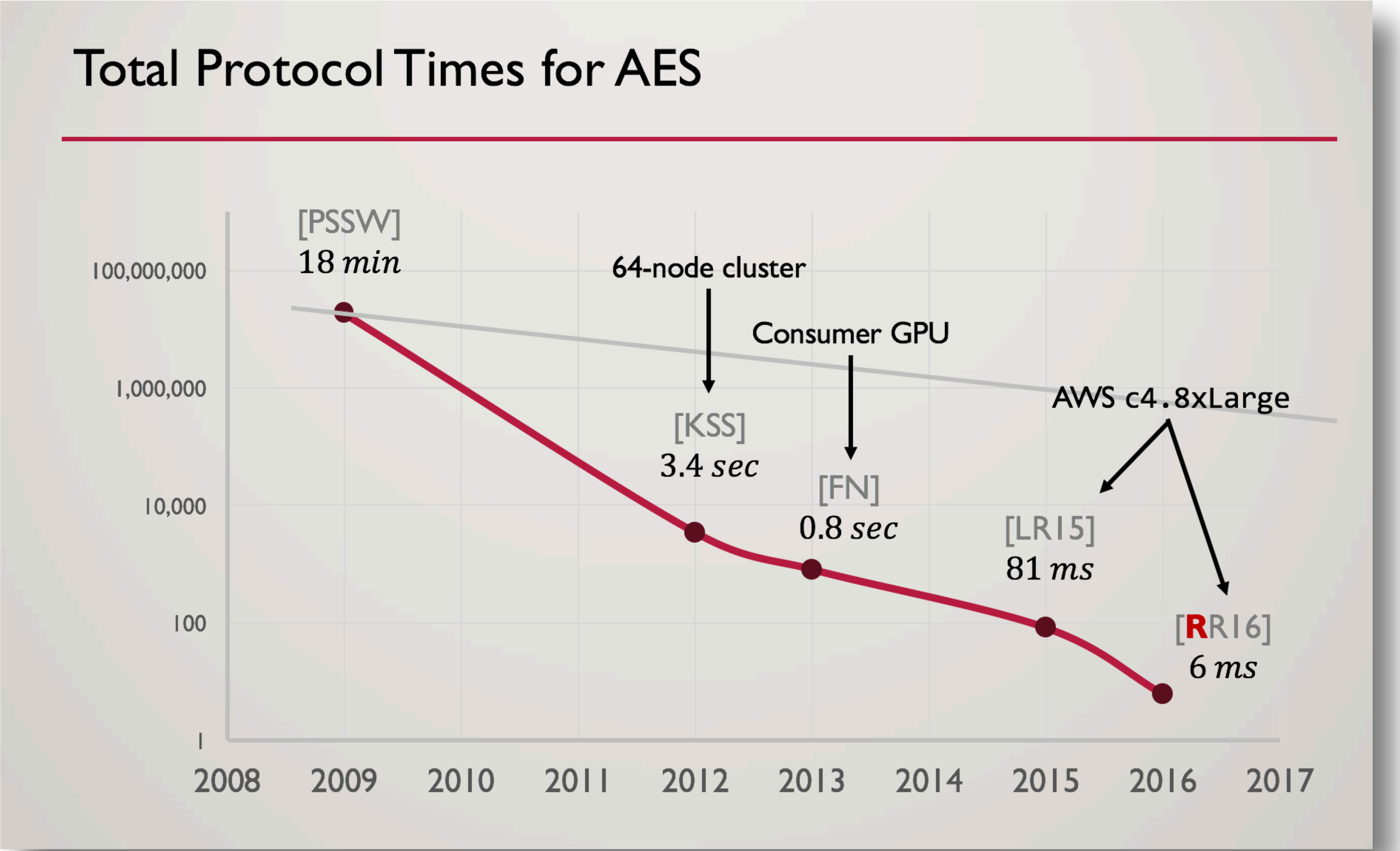
Secure Computation: Progress, Challenges, and Open Questions

NSF SaTC Pis Meeting 2017
Breakout Session #11

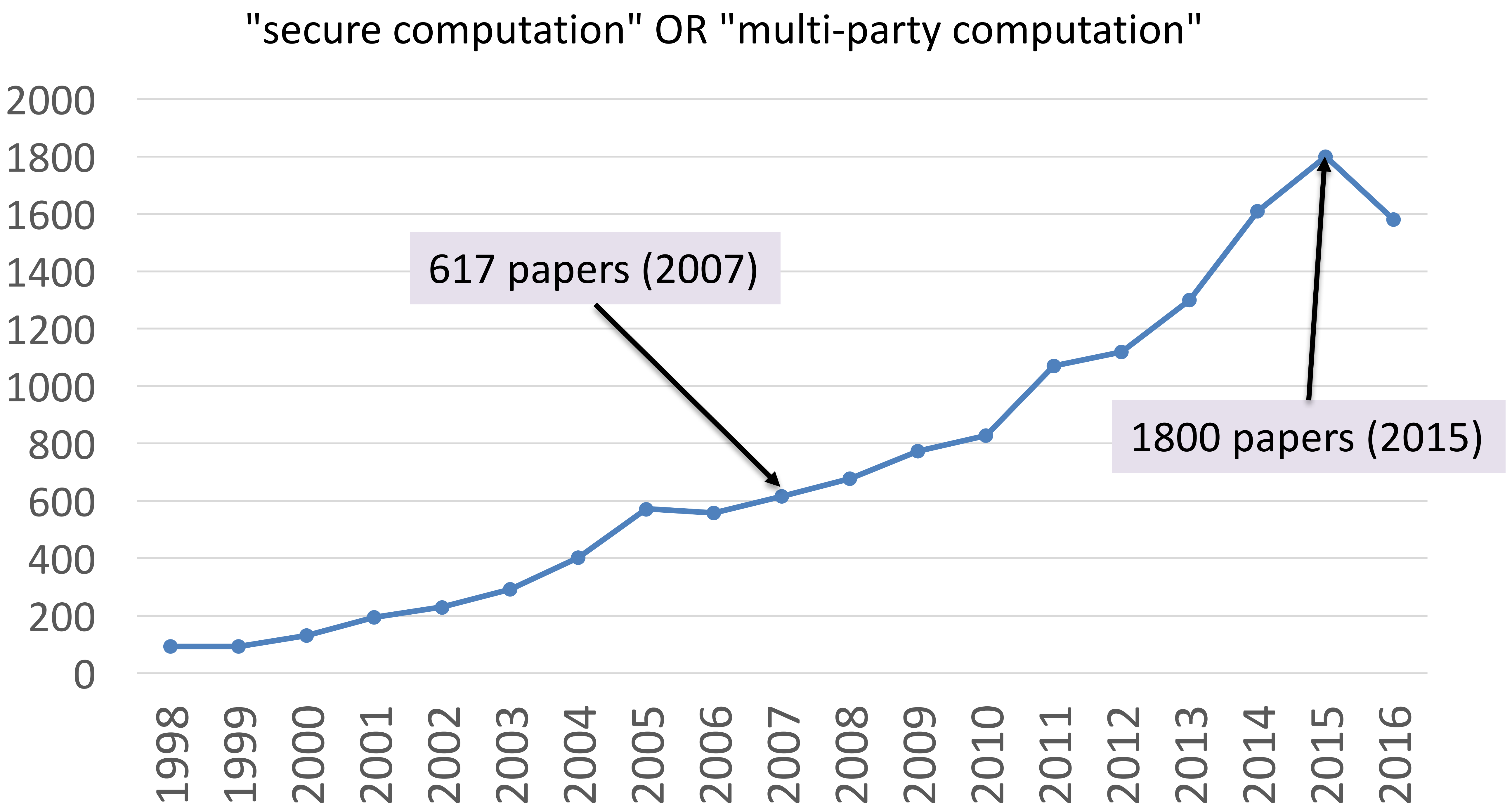
David Evans
https://www.cs.virginia.edu/evans

Decade of Remarkable Progress!



Total Protocol Times for AES

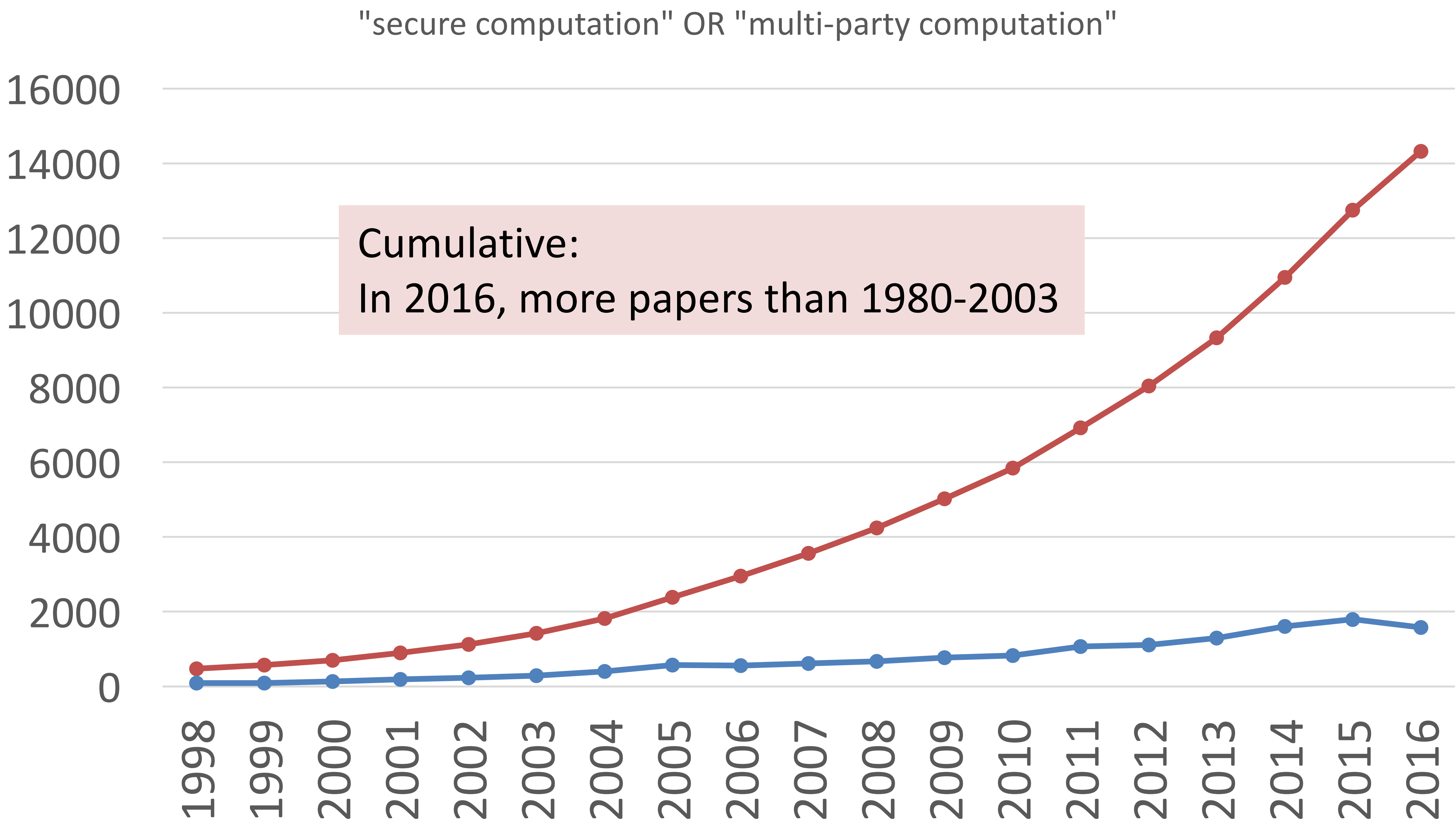
Slide from:
Peter Rindal
Mike Rosulek
(USNEIX Sec
2016 talk)



"secure computation" OR "multi-party computation"

617 papers (2007)

1800 papers (2015)



Cumulative:
In 2016, more papers than 1980-2003

Dozens of Tools and Libraries

Proliferation of Threat Models

- **Active**
  - Malicious
  - Covert
  - One-bit leakage
- **Passive**
  - Semi-honest

- **"Semi-Trusted" parties**
  - Two+ non-colluding
  - Correlated randomness providers
- **Majority Honest**
- **Fairness**
- **Trusted Hardware (e.g., SGX)**

Should we be inventing more? Standardizing on a few?
How important is it to motivate threat models by real problems?

Metrics

- Feasible Scale
- On-line/Off-line; Pre-processor
- Latency – Local/LAN/WAN
- Cost / Throughput

Which ones matter?

Benchmarks

- Private Encryption (AES, RSA)
- Graph algorithms
- Genomics
- Stable matching
- Privacy-preserving machine learning

Deployments

- Beet Auctions
- Boston Wage Study
- Key-Splitting
- Data analysis
- Encrypted Databases

Capabilities have changed 1Mx – but same applications at 2007?

Open Questions

- How should we be **connecting MPC with privacy**?
- How to establish **end-to-end trusted toolchains**?
- How can **trust be conveyed** meaningfully to data owners?
- What are the **compelling applications**?
- What are the **important open theoretical questions**?