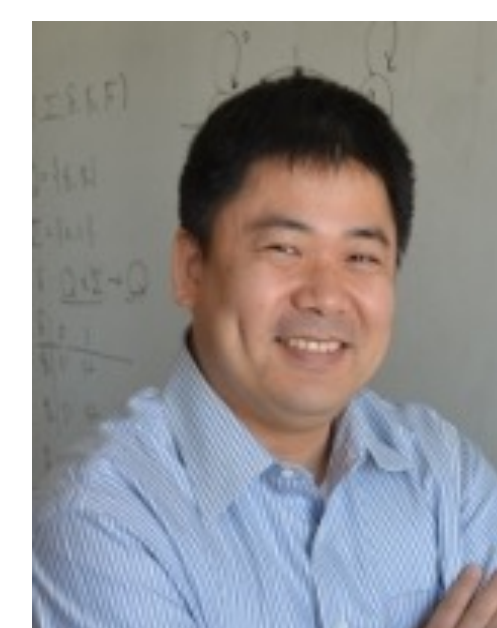


New Approaches for Large Scale Secure Computation

Arkady Yerukhimovich – George Washington University,
S. Dov Gordon – George Mason University,
Seung Geol Choi – U.S. Naval Academy



Challenge:

To develop new tools and protocols for facilitating large-scale, distributed, secure computation.

- Millions of parties
- With varying resources
- With realistic network constraints

Scientific Impact:

- Improved large-scale MPC will enable citizens to collaboratively leverage their data, while protecting individuals from third party observation.
- General approaches for large-scale MPC will lead to new applications
- Asymptotic improvements help identify what resources are necessary for achieving large-scale secure computation.
- Relaxed models supporting real computing environments help researchers explore new tradeoffs between privacy and efficiency.

Technical Approach:

- New MPC protocols with improved asymptotic costs.
 - Honest-majority MPC with decreasing cost as more parties join.
 - Malicious-majority MPC with constant per-party cost.
- New security models and protocols for handling failed parties, and dynamic participation.

- Improved protocols for specific computations: multi-party set intersection, and distributed data shuffling.
- Oblivious data-structures for privacy-preserving fake news detection in encrypted messaging systems

Broader Impact (impact on society – who will care)

- Citizens, corporations and governments are becoming concerned with data privacy.
- Fighting fake news in encrypted messaging will help stem the flow of fake news in such platforms.

Broader Impact (education and outreach)

- Training graduate students and postdocs in MPC research.
- Teaching MPC protocol development to undergraduate and graduate students.
- Leading outreach on MPC to community college instructors

