NSF Grant Proposal Experience for Work on Secure Computation and Outsourcing

Marina Blanton

Department of Computer Science and Engineering

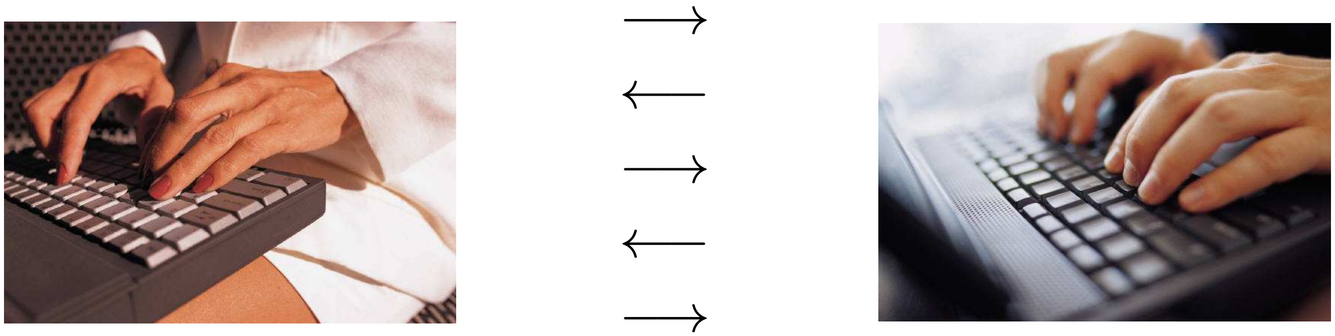
University of Notre Dame

NFS/DIMACS Workshop for Aspiring PIs in Secure and Trustworthy Cyberspace

August 17, 2014

My Area: Secure Computation and Outsourcing

- Secure collaborative computation allows two or more parties to evaluate a function on their private inputs
  - the parties obtain their outputs, but no other information is revealed
  - similar to as if the computation was performed by a trusted third party



Alice

Bob

Secure Computation

- Work on secure multi-party computation began in early 1980s and continues today
- It has been long known that any function can be securely evaluated with provable security guarantees
- Recent work targets
  - optimizing performance of general-purpose techniques
  - optimizing performance of commonly used building blocks (e.g., integer comparison)
  - building custom optimized protocols for specific functions

Secure Computation Outsourcing

- Cloud computing enables convenient on-demand access to computing or storage resources
- Security and privacy considerations, however, stand in the way of its full utilization
  - the computation may be corrupt or skipped
  - sensitive data may be leaked
- Secure computation outsourcing allows computation to be carried out by a cloud provider on protected data without revealing anything about the data or computation results
- Verifiable outsourcing allows the integrity of the computation (i.e., correctness of the result) to be verified at low cost

Current NSF-Funded Projects

- **Project 1: Securely computing with biometric data**
  - covers secure two- and multi-party computation techniques for computing with biometric data
  - covers secure outsourcing of biometric processing as well as efficient techniques for verifying correctness of the result
  - covers a number of biometric modalities (such as iris, fingerprints, voice, and DNA)
  - treats diverse biometric representations and algorithms for different stages of biometric processing

Current NSF-Funded Projects

- **Project 2: Toolset for general-purpose computation and outsourcing**
  - **targets design and development of secure techniques for enabling efficient execution of a general-purpose program**
    - **techniques are suitable for both secure collaborative computation and secure computation outsourcing**
  - **the project components are**
    - **secure arithmetic for standard data types (floating point, strings, etc.)**
    - **data-oblivious algorithms and data structures**
    - **compiler that translates a C program with data to be protected marked as private into its secure distributed implementation**

From a Proposal to a Grant

- **My experience with NSF proposals:**
  - **other people's proposal writing style may not work for you**
  - **including multiple preliminary results was perceived better than a single result**
  - **continuing to work on the project prior to resubmitting the proposal was helpful**

What does It Take to Get a Proposal Funded?

- Interesting research idea
- Providing mechanisms for implementing the idea and preliminary results
  - at least one publication or publishable result
  - put your best work forward
- Solid integration of project components
- Proper project scope
- Persistence
- Using help