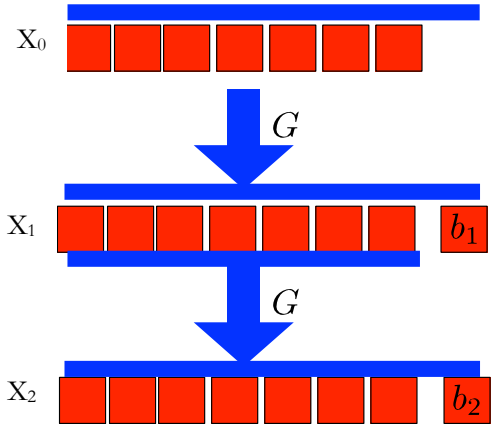
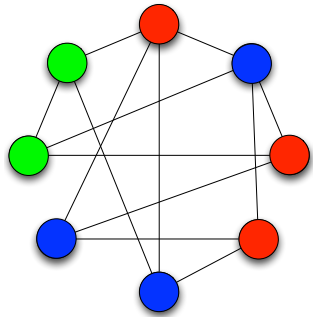
Cryptography Research Group





Our group is working on the problem of secure two-party computation. This primitive allows two parties, one with input x and another with input y, to compute an arbitrary function f(x,y) of their inputs in such a way that neither party learns anything other than f(x,y). In other words, no intermediate information about their private inputs is leaked. These types of primitives enable various collaboration scenarios between entities that do not want to share their private information but still want to collaborate. We currently have one of the world's fastest systems for performing these types of computations.

Abhi Shelat

Assistant Professor
shelat@cs.virginia.edu
www.cs.virginia.edu/~shelat

Department of Computer Science
University of Virginia
Charlottesville, VA
434.243.2145

"Expanding the use of cryptography to information privacy and security in a societal acceptable manner."

UNIVERSITY of VIRGINIA
ENGINEERING

Cryptography

Balancing the need for public information disclosure for accountability with the need to conceal for privacy is a societal challenge. We are working to address that balancing act by replacing – at the societal level – disclosure protocols by more nuanced cryptographic ones. In particular, the theory of zero-knowledge protocols allows an organization to counter-intuitively prove properties about its internal condition without disclosing much private information about it. We seek to overcome the challenges which stymie the use of such cryptography to promote organizational legitimacy without the invasion of privacy.

Security

We are exploring the fundamental open problems concerning security notions for fully homomorphic encryption. Specifically, we are research the relationship between fully homomorphic encryption and CCA2-secure encryption. We are also designing methods to build stronger notions of fully homomorphic encryption. Lastly, we are interested in applying homomorphic encryption to construct secure function evaluation protocols that tolerate malicious adversaries but still enjoy low communication complexity.

RECENT RESEARCH DEVELOPMENTS

- Our team has introduced the concept of renegotiation-safe equilibrium. This concept is a useful game-theoretic notion and also provides the best way of modeling parties with limited computational resources in cryptographic protocols.
- Developed the fastest platform for two-party secure computation. Our system allows two mutually distrustful parties, each with private inputs x and y respectively, to jointly computer a function f(x,y) in a manner that the parties only learn the output (and what they can deduce from their private input and output).

RECENT GRANTS

- DOD/Air Force-Minimizing Overhead for Secure Multiparty Computation and Fully Homomorphic Encryption
- NSF/CAREER-Legitimacy through Cryptography

SEAS Research Information
Pamela M. Norris, Associate Dean
University of Virginia
Box 400242
Charlottesville, VA 22903
pamela@virginia.edu
434.243.7683

UNIVERSITY of VIRGINIA
ENGINEERING