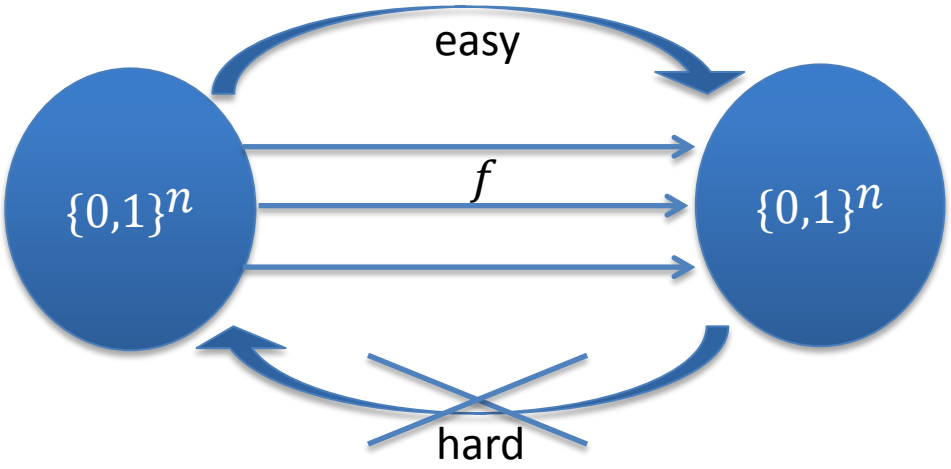

We work on foundations of cryptography, a field that aims at designing cryptographic protocols with provable security. As a result our research is tightly related to the field of computational complexity which provides the framework for such studies.

Cryptography & Computational Complexity Research Group

Mohammad Mahmoody

Assistant Professor
mohammad@cs.virginia.edu
www.cs.virginia.edu/people/faculty/mohammad.html

Department of Computer Science
University of Virginia
Charlottesville, VA
434.982.2989

"Building secure cryptographic systems on firm foundations through a mathematical study of physical and computational assumptions.

UNIVERSITY of VIRGINIA

SCHOOL of ENGINEERING & APPLIED SCIENCE

Cryptography

- Can we base the security of cryptographic schemes on the hardness of the Travelling-Salesman problem (i.e. achieving NP-hard security)?
- How efficient could cryptographic schemes be when we use the more believable and well-studied forms of assumptions to design and prove them secure?
- How powerful are our "proof-methods" (e.g., black-box vs. non-black-box, classical vs. quantum, etc.) in theory of cryptography?

The above are examples of fundamental questions about "computational assumptions" behind cryptographic systems. We study the power and limitation of computational assumptions in cryptography and their internal relation. The goal of this research is to build cryptography on a *minimal* set of assumptions. We also study the other type of assumptions regarding the *physical* aspects of a designed secure system. For example, we study the power and limitations of tamper-proof hardware in cryptography as well as (possibility or impossibility of) cryptographic schemes with tamperable randomness.

Computational Complexity

Our approach to computational complexity theory is to better understand the hardness and complexity of computational tasks and assumptions---both known as "primitives"---in cryptography. For example, what would be the complexity theoretic implications of building encryption schemes with NP-hard security? Or more generally, what is the computational complexity of breaking specific cryptographic primitives/tasks such as collision-resistant hash functions, homomorphic encryption, etc.? We also work on importing ideas and tools (e.g., probabilistically checkable proofs) to base cryptography on tamper-proof hardware.

RECENT RESEARCH DEVELOPMENTS WIH COLLEAGUES

- Proving the impossibility of cryptography using tamperable randomness.
- Proving lower bounds on the computational assumptions behind (indistinguishability) code obfuscation.
- Proving lower bounds on idealized models for virtual black-box code obfuscation.

RECENT GRANTS

- NSF CAREER award 2014.

SEAS Research Information
Pamela M. Norris,
Executive Associate Dean for Research
University of Virginia
Box 400232
Charlottesville, VA 22903
EngineeringResearch@virginia.edu
434.243.7683

UNIVERSITY of VIRGINIA | SCHOOL of ENGINEERING & APPLIED SCIENCE