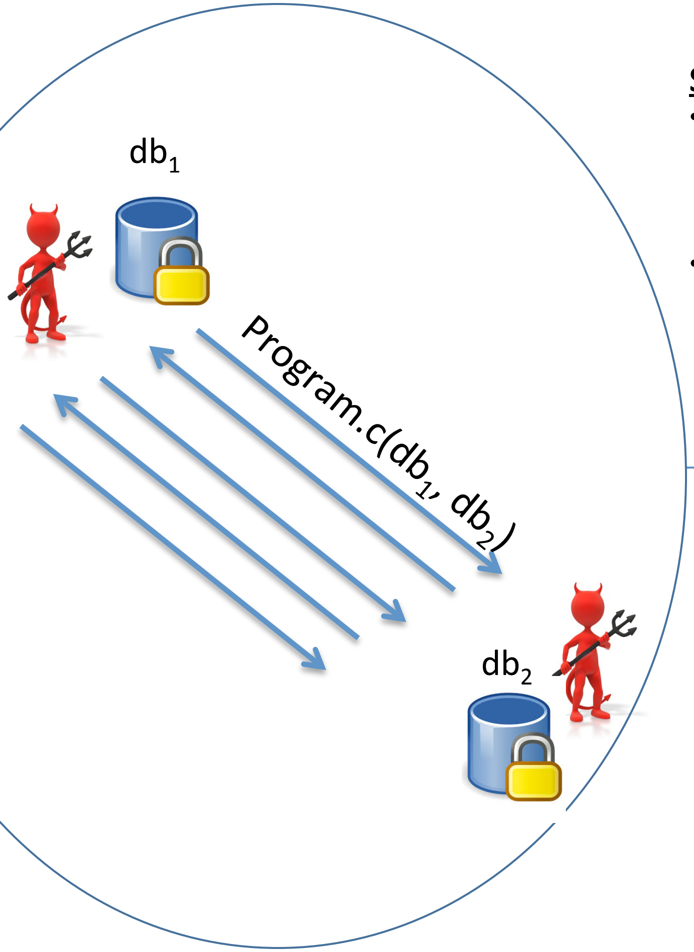
New Protocols and Systems for RAM-Based Secure Computation

Challenge:

When computing on encrypted data, the access pattern to memory can leak a lot of information. Generic approaches for building data oblivious algorithms are costly. We need automated methods for building tailored, data oblivious algorithms.



Solution:

- We have developed a new ORAM protocol for the 2 server setting, useful for secure computation.
- We have developed new security notions that balance privacy with efficiency.
- We have identified various classes of computation that can be handled more efficiently than arbitrary polynomial-time computation.
- We designed a sound programming language for expressing oblivious computation.

Award # 1564088, 1563722, 1562888

S. D. Gordon, M.Raykova, J.Katz, M.Hicks, R. Piskac
GMU, UMD, Yale

Scientific Impact:

- Our research provides new techniques for computing on encrypted data, facilitating collaboration while maintaining privacy.
- Our work provides insight into what information is leaked through memory access patterns, and provides several new mechanisms for defending against such leakage.

Broader Impact:

- Techniques for computing on encrypted data have the potential to impact government agencies and corporations holding sensitive user data.
- Code has been made available, which we hope will help move these techniques from theory to practice.
- We have involved postdocs, graduate students, and undergraduate students in this research.