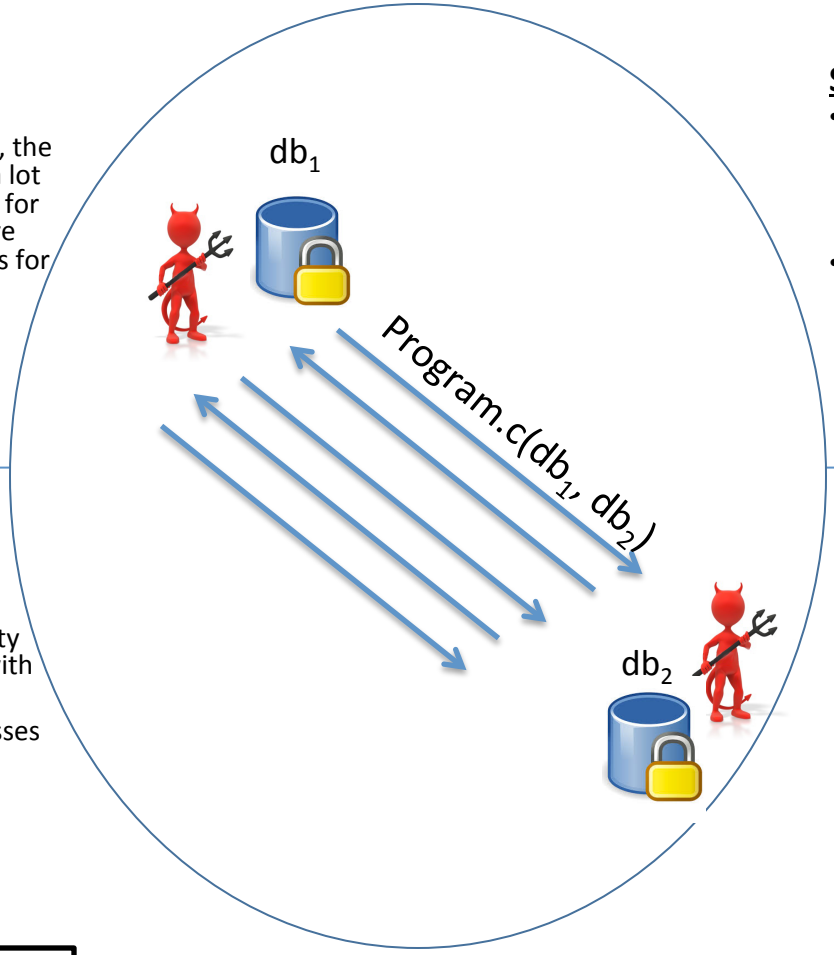
New Protocols and Systems for RAM-Based Secure Computation

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 are developing new data structures to facilitate data oblivious computation.
- We are developing new security notions that balance privacy with efficiency.
- We are looking for various classes of computation that can be handled more efficiently than arbitrary polynomial-time computation.

Scientific Impact:

- Our research will provide new techniques for computing on encrypted data, facilitating collaboration while maintaining privacy.
- Our work will provide insight into what information is leaked through the memory access patterns, and a toolkit 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 will be made available; our framework will help move these techniques from theory to practice.
- We are involving postdocs, graduate students,, and undergraduate students in the research.
- We will be developing new courses on secure computation.

Award # 1564088
S. D. Gordon, M.Raykova, J.Katz, M.Hicks
GMU, UMD, Yale