Research Assistants Needed

We are looking for students to work as RAs in the Crypto@RIT research group. The RAs will contribute to the development of a prototyping and evaluation framework, and implementation of Homomorphic Encryption (HE) schemes [1]. Prior understanding of HE is not required, but background in cryptography is essential. For example, students who have taken the Foundation of Cryptography, Advanced Cryptography, or other similar courses, are welcome.

The RAs should have the following experience or skills:

- 1+ years of C/C++ programming experience.
- Linux program development.
- Experience with some Linux toolchains, such as Autotool, CMake.
- Git version control experience is a plus.

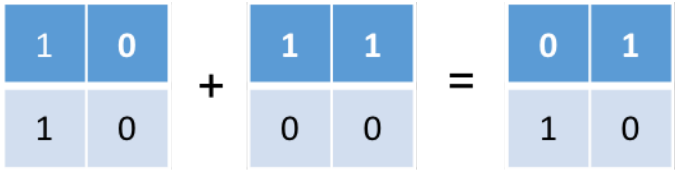
Upon joining our group, the RAs will work on one or more of these tasks:

- Learn FLINT, a C++ library for Number Theory
- Port our HE framework over to use FLINT
- Prepare unit-tests for the framework and the HE schemes

The implementation involves heavy use of vectors and matrices. If you are interested in this RA position, please email me (ph@cs.rit.edu) your code (in C/C++) solving the following programming exercise. Please include Autotool or Cmake files, or at least a makefile, for me to test it.

1. Create two 10x10 matrices and populate them with random value of 0 or 1.
2. Apply *coordinate-wise* addition, XNOR, subtraction and multiplication using these matrices.

   See the following example for a sample 2x2 coordinate-wise addition.



[1] Daniele Micciancio. *A first glimpse of cryptography's Holy Grail*. ACM Communication. 2010.