# Computer Science Colloquium

**Thursday, April 2, 2015**

**9:30 am-10:30 am**

**Research Hall 163**

## Practice-Oriented Cryptography: A Definition-Centric Approach

In cryptography, a good formalization can often lead to significant improvements for both security and efficiency. In this talk, Dr. Hoang will discuss two illustrative examples.

First, I'll present UCE, a security model for hash functions (a very widely used operation in cryptography) that gives rigorous justification for several important heuristic schemes.

While UCE can be directly instantiated via existing hash constructions, which are already quite efficient, I'll show a novel hash design that leads to extremely fast instantiations of UCE.

Second, I'll give the first formalization of garbled circuits, a central technique in cryptography. Based on this abstraction, I discover critical bugs in several well-known applications and implementations. I also present new optimization methods that significantly improve the speed of creating and evaluating garbled circuits.

## Viet Tung Hoang

Biography

Viet Tung Hoang is a postdoc at Georgetown University (with Adam O'Neill) and University of Maryland College Park (with Jonathan Katz).

He did his Ph.D. at UC Davis under the supervision of Phillip Rogaway, and then spent another year doing a postdoc at UCSD with Mihir Bellare.