1161-68-148 **Susan Hohenberger*** (susan@cs.jhu.edu), **Venkata Koppula** and **Brent Waters**. *Building Secure Encryption from a Simple Function.*

Chosen-ciphertext attack (CCA) security is the de facto standard for public key encryption. The cryptographic community has had success in realizing CCA secure encryption from a variety of number-theoretic assumptions. This success encouraged a strong drive to realize CCA secure encryption from a general assumption, such as injective trapdoor functions. A trapdoor function is a primitive in which any user given a public key PK can evaluate an input x by calling $F_{eval}(PK, x) = y$. And a user with the secret key SK can recover x from y as $F_{inverse}(SK, y) = x$. However, a polynomial-time attacker without the secret key should not be able to output x given $F_{eval}(PK, x) = y$ for a randomly chosen x. By injective, we require a one-to-one mapping of the function input and evaluation spaces.

In this talk, I will present a construction of CCA secure public-key encryption from injective trapdoor functions. The construction is black box and assumes no special properties (e.g. “lossy”, “correlated product secure”) of the trapdoor function. This result is joint work with Venkata Koppula and Brent Waters. It was recognized with a Best Paper Award at CRYPTO 2020. (Received August 15, 2020)