Why is it hard to base OWFs on complexity-theoretic assumptions?

Felix Rohrbach
TU Darmstadt

Abstract:

While it is commonly believed that one-way functions (or cryptography in general) exist, we have yet failed to prove their existence on any popular complexity-theoretic assumption, as for example P!=NP or the existence of average-case hard problems. This has famously been captured by Impagliazzo in his five worlds, which describe different possible realities regarding the existence of hard problems.

In this talk, I will present a technique called Relativized Separations that can be used to rule out commonly used proof techniques for a given question in complexity theory. This technique has been used to show that, indeed, it is hard to prove that we do not live in one of Impagliazzo's worlds without one-way functions.

**

Felix Rohrbach works on cryptography and its relation to complexity theory. He is a PhD student of Marc Fischlin and located at TU Darmstadt, Germany.

Time: Monday, 9 March at 14:00-15:00 (We start at 14:00 sharp :-) )
Location: U149 U6 KONECRANES, Otakaari 1