CSE Seminar Series
Wednesday, February 28 at 11:30am, NTDP F285

Code-Based Cryptography for Post-Quantum Standardization

Dr. Edoardo Persichetti

Abstract
Code-Based Cryptography is one of the most promising families within the so-called Post-Quantum Cryptography. This area of research stems from the need to address the possible threat posed by Quantum computers. In fact, thanks to Shor's Algorithm, the majority of cryptographic primitives in use today (based on "classic" Number Theory problems such as factoring or computing discrete logarithms) will be insecure once a suitable quantum computer is developed. Therefore, it is necessary to provide credible alternatives and be ready for a major change. Keeping in mind migration time and the desired lifetime of secrets, it is clear that it is already time to move, and with this in mind, NIST has launched a call for proposals to design the new standards for Post-Quantum cryptography.
In this talk, I will discuss some recent developments in Code-Based Cryptography. After introducing and reviewing the primitive known as KEM (Key Encapsulation Mechanism), I will present three projects that have been submitted as candidates for NIST's call. Everyone welcome!

Bio
Dr. Edoardo Persichetti is currently an Assistant Professor in the Department of Mathematical Sciences at Florida Atlantic University. Before moving to Florida, he was Assistant Professor of Mathematics at Dakota State University and Postdoc (Adiunkt Naukowy) in the Cryptography and Data Security Group at Warsaw University in Poland. He completed his PhD in Mathematics in late 2012 at University of Auckland, New Zealand under the supervision of Steven Galbraith. His research interests are public-key cryptography (post-quantum, provable security) and number theory (mainly coding theory), with several papers published in top-tier conferences in cryptography such as PKC, ACNS and PQCrypto, as well as journals like the Journal of Mathematical Cryptology. Dr. Persichetti has served as peer-reviewer for many internationally-recognized conferences and is currently serving as editor for the IACR Book Reviews system.