UNIVERSITÀ DI PISA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Dottorato di Ricerca in Ingegneria dell'Informazione

Doctoral Course

"An Introduction to Post-Quantum Lattice-Based Cryptography"

Dr. Pericle Perazzo

Dept. of Information Engineering – University of Pisa – Italy

Short Abstract: Imagine that, few years from now, someone announces that a large-scale quantum computer has been successfully built. The next day, the New York Times claims that all the encrypted communications on the Internet are broken, and public opinion breaks into panic. Post-Quantum Cryptography (PQC) includes all those cryptosystems that are believed to be resistant against attacks by both classical computers and quantum computers. PQC is paramount to avoid the catastrophic scenario said before.

In this PhD course we will introduce the most promising family of PQC, namely Lattice-Based Cryptography.

Course Contents in brief:

- Introduction to Post-Quantum Cryptography (Grover's algorithm, Shor's algorithm, PQC families)
- Lattice problems (SVP)
- Lattice-based hashes (Ajtai's construction)
- Lattice-based encryption schemes (Goldreich-Goldwasser-Halevi scheme, NTRU scheme)
- LWE-based encryption schemes

Total # of hours of lecture: 12

References:

[1] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen. 2008. Post Quantum Cryptography (1st. ed.). Springer Publishing Company, Incorporated.

CV of the Teacher

Pericle Perazzo received the Master degree cum laude in Computer Engineering in 2010 and the Ph.D. degree in Information Engineering in 2014, both from the University of Pisa, Italy. During his Ph.D. studies, he has been Visiting Researcher in the Institute for Parallel and Distributed Systems (IPVS) of Stuttgart, Germany. Since 2017, he has been Researcher at the Department of Information Engineering at the University of Pisa. His research interests include the area of security and privacy in the Internet of Things, with special emphasis on secure localization, attribute-based encryption, blockchain technologies, and post-quantum cryptography.

Room and Schedule

Room: *Aula Riunioni del Dipartimento di Ingegneria dell'Informazione, Largo Lucio Lazzarino 1, Pisa*

Schedule:

Day1 – 3 hours

Day2 – 3 hours

Day3 – 3 hours

Day4 – 3 hours (including final exam)