Department of Computer Science

Why designing and implementing encrypted search is hard?

Zichen Gui
ETH Zurich

Hosted by Reza Curtmola

Date: Wednesday, April 10, 2024
Coffee: 2:15 PM – 2:30 PM
Time: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
Webex link: https://njit.webex.com/njit/j.php?MTID=m6525c4fcaf47f9752d3490fbe89daf35

Abstract:
Encrypted search is the study of cryptographic algorithms that allow users to efficiently search over encrypted data they store on cloud servers. Since the introduction of encrypted search in 2000, the field has received a lot of attention from the community and enjoyed significant progress in terms of search functionalities and efficiency. However, there is yet not a single encrypted search product that is expressive and efficient enough on the market to replace unencrypted database management systems.

In this talk, we will take a deep dive into the design of encrypted search algorithms and try to understand the challenges involved in the process. We will also show that securely implementing an encrypted search algorithm in the real world is far from trivial using Queryable Encryption from MongoDB as a case study.

Bio:
Zichen Gui is a postdoctoral researcher in the Applied Cryptography Group at ETH Zurich. He completed his Ph.D. at the University of Bristol in 2022. His research focuses on different aspects of encrypted search, including theoretical foundation, construction and cryptanalysis of encrypted search algorithms.