

# Research Topics

Formal Methods for Information Security

Morteza Amini

15 Aban 1391

The research topics are but not limited as follows:

- Logic-based access control
- Formalizing privacy
- Logical specification and reasoning about obligations
- Formal methods to source code security evaluation and assurance
- Secure programming using type systems
- Foundations of compositional security (formal specification and reasoning)
- Verification of security protocols (techniques, tools, etc.)
- Techniques and tools for verification of access control mechanisms against the models

## **Important Dates:**

- Research proposal: 91-08-25  
The title, brief abstract and group members should be emailed to amini[AT]sharif
- Oral presentation: Last 2 or 3 sessions of the class  
Understanding and introducing the research done in the chosen topic is important. You are not supposed to have contribution or have an overall survey. The presentations should be in-depth enough; however, they should not be seemed complex for student to understand.