# 北陸先端科学技術大学院大学研究室教育指針
# Laboratory Education Guideline

研究室教育指針は、学則第３０条の３に基づき、研究指導の方法及び内容並びに修了までの研究指導の計画をあらかじめ明示するものです。
Based on the Article 30-3 of the general academic rules, the Laboratory Education Guideline is intended to clearly outline the methods and content of research guidance, as well as the plan for research guidance until completion.

氏名 / name： FUJISAKI Eiichiro　　役職 / official position： Professor

1. 研究テーマ / Research Theme

Cryptography and Information Security. In particular, research on theoretical cryptography, post quantum cryptography, cryptographic protocols, and multi-party computation.

2. 修得が期待される能力 / Competencies expected to be acquired

研究室教育は必修 A 科目（先端）又は研究支援科目（融合）の一部として単位化されており、この欄はそれら科目のシラバス上の達成目標の一部となります。
Laboratory Education is accredited as a part of the Required courses A (Division of Advanced Science and Technology) or Research Support Courses (Division of Transdisciplinary Sciences), and this section constitutes a part of the course goals stated in the syllabus for such subjects.

Students are expected to acquire knowledge of cryptographic algorithm design and the theory of security proofs for cryptographic protocols. This knowledge enables them to take a comprehensive view of information system security and to derive fundamental, non-ad hoc solutions to vulnerabilities and flaws in protocols. In addition, students will develop the necessary mathematical foundations – such as linear algebra, number theory, and statistics – required to understand these topics. Depending on the theme, they are also expected to gain knowledge of quantum computation and cryptanalysis.

3. 研究指導方針 / Research Guiding Principle

Our laboratory aims to educate and train future outstanding researchers and developers in cryptography and information security. We support students in acquiring fundamental knowledge of cryptographic theory and the mathematical background necessary for its understanding through seminars, reading groups, and formal courses, while encouraging them to develop independence in conducting research. As the final stage of the fundamental research cycle, presenting research results at academic conferences is essential, and we strongly encourage external conference presentations of master's research. In particular, doctoral students are required to present their research outcomes in English.

4. 研究室活動の内容及び方法 / Content and Methods of Laboratory Activities

□日次活動 / Daily Activities：
□週次活動 / Weekly Activities： Student-led reading seminars on textbooks and research papers, as well as individual supervision meetings.
□月次活動 / Monthly Activities：
□不定期活動 / Occasional Activities： Schedule coordination via Slack, and announcements of external events.

5. 年間スケジュール / Annual Schedule

本学の全学共通の年間スケジュールは「履修案内」の「学位取得に至るスケジュール」を参照してください。（本学HP 参照：ホーム＞教育＞履修関係＞履修案内）
Please refer to the "Degree conferment schedule for the master's program/doctoral program" in the "Degree Completion Guide" for university-wide common schedule (JAIST website: Home >Education>Taking Courses>Degree Completion Guide)

**Master's Program:**

After joining the laboratory, students are expected to participate immediately in student-centered reading groups. For students who wish to join the laboratory, participation is recommended even before formal assignment. For students who begin research in this field after entering graduate school, we strongly recommend making use of the *M-alpha* program.

By approximately six months after joining the laboratory, students are expected to have largely determined the topic of their master's thesis.

*Midterm Presentation:*

In principle, all students are required to give a midterm presentation. At this stage, students are expected to have acquired sufficient knowledge of their research topic and to have identified a reasonable direction toward solving their research problem.

*December in the final year:*

Students are expected to complete the first draft of their master's thesis by mid-December and are strongly encouraged to present the same work at the *SCIS Symposium on Cryptography and Information Security*, organized annually by the Institute of Electronics, Information and Communication Engineers (IEICE) in January. If this is not feasible due to progress or other circumstances, students are expected to present their work at a later IEICE or Information Processing Society of Japan (IPSJ) technical meeting.

Doctor Program:

During the doctoral program, students are expected to aim for at least two international conference presentations and one or more journal publications. In particular, students should present their research at an international conference by the end of the second year (D2) and subsequently submit the results as a journal paper. In the third year (D3), students are expected to submit and present a different research outcome at an international conference. These research results are then compiled into the doctoral dissertation.