# 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： 藤崎 英一郎 役職 / official position： 教授

| |
|---|
| 1. 研究テーマ / Research Theme |
| 暗号・情報セキュリティ．特に暗号理論，耐量子公開鍵暗号，暗号プロトコル，秘密計算アルゴリズム等 |
| 2. 修得が期待される能力 / Competencies expected to be acquired<br>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。<br>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. |
| 暗号アルゴリズムの設計法や暗号プロトコルの安全性証明理論の修得が期待できる．これらの知識は情報システムのセキュリティを俯瞰し，脆弱性，プロトコルの欠陥などに対して対処療法でない本質的な解決策を導くことに役立つ．またそれらを理解するために必要な線型代数，初等整数論，統計などの数学的知識の修得．またテーマに応じて量子計算や暗号解読技術の修得が期待できる． |
| 3. 研究指導方針 / Research Guiding Principle |
| 本研究室では，将来の優秀な暗号や情報セキュリティの研究者・開発者を育成することを目標にしている．暗号理論の基礎とその理解に必要な数学的知識の修得をゼミ，輪講，単位科目などを通じてサポートしながら，研究者に必要な主体性をもち研究を進める能力をもつ学生を育成することを目指す．研究の基本サイクルの最後として，学会での発表は重要であり修士研究の外部発表を強く推奨している．特に博士後期課程学生は英語で研究成果を発表することを義務付けている． |
| 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：<br>□週次活動 / Weekly Activities： 学生を中心とした教科書や論文の輪講，個別の研究テーマに関するゼミ．<br>□月次活動 / Monthly Activities：<br>□不定期活動 / Occasional Activities： Slack を用いたスケジュール管理．外部イベントの紹介など． |
| 5. 年間スケジュール / Annual Schedule<br>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）<br>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) |
| **博士前期課程**<br>配属後，直ちに学生中心の輪講に参加（配属希望者には，配属前から参加を推奨）．大学院に入ってからこの分野の研究を始める学生に対しては M alpha 制度を利用することを強く推奨．配属半年経過時点で修論のテーマをある程度確定することを目指す．<br>中間発表：原則発表．その時点で研究テーマへの十分な知識と解決への道筋がある程度見えていることを目指す．<br>修士論文の最初のドラフトを１２月中旬までに書き上げることを目標とし，同内容を |

毎年１月に行われる電子情報通信学会主催の「SCIS 暗号と情報セキュリティシンポジウム」で発表することを強く推奨する．進捗等の関係で無理な場合もその後の電子情報通信学会，または情報処理学会の研究会で発表を行うこと目指す．

**博士後期課程**

博士後期課程在学中に国際会議発表２件，ジャーナル論文１件以上を目指す．特に D2 までの間に国際会議で発表し，その結果をジャーナル論文に投稿できるようにする．
D3 では別の研究成果を国際会議に投稿し発表する．これらの研究成果を博士論文にまとめる．