Exam

Name: ______________________ ID: ______________________

This assignment has **2** questions, for a total of **75** marks.

Question 1: **Explain** . . . . 25 marks

Describe one of the following topics that we presented in class in a lecture-notes style. Provide examples, intuitions and concise explanations. Guide the reader to understand why a certain topic is important. Present the key technical details that are needed to understand the topic in an organic way.

Try to keep the presentation to 2-3 pages in "report" format, in case of lengthy formulas, you can use up to two more pages.

Preface these notes with a short explanation (1/2 a page) of the motivations and goals behind the secure compilation research field.

Topics:

1. the precise backtranslation between the pure typed and the pure untyped languages: what is the backtranslation type, why do we need inject and extract, what properties do we need of it;
2. fully abstract compilation: why does it have security relevance, how can we prove it, pros and cons;
3. fully abstract compiler between the pure languages and between the pure language and the assembly language: what do we need to attain FAC, how do we attain FAC;
4. contextual equivalence: how can we use it to encode security properties;
5. trace-based backtranslation between the pure typed and the pure untyped languages: why do we need it, how do we define it;
6. trace semantics: why do we need them, what do they capture, what properties do we need of them for FAC;
7. robust compilation: why do they have security relevance, why do we have equivalent criteria, what proof techniques apply to what criteria;
8. robustly-safe compilation between the impure language and the impure, capability-enhanced language: what kind of backtranslation do we need, what does the compiler need to do;
9. comparison between FAC and RSC in the concrete case of compiling between the impure languages: what complicates in the traces, what complicates in the backtranslation, what must the compilers do differently and why;
10. traces as security specifications: how can they encode security properties, different kinds of traces for security and proof devices;
11. context-based backtranslation between the stateful languages and how to use it to prove RTP and RHP, when are different kinds of backtranslation applicable and why.

Question 2: **Further Inquiries** . . . . 50 marks

The oral examination will take it from your previous answer.