AARHUS UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

Bachelor Contract
Date: March 24, 2019
Page 1/1

| | |
|---|---|
| **Advisor** | Bas Spitters |
| **Students** | Kira Kutscher |
| **Languages** | English |
| **Text tools** | LaTeX |
| **Other tools** | Coq |

## Project Description

The project will focus on developing a framework for cryptographic proofs in Coq. We will investigate how much of the convenience found in tools like cryptHOL (for Isablle) or Easycrypt we can recreate within the more powerful logic of Coq. To this end we will first investigate existing tools (like the above mentioned) and libraries/tools for Coq that might be of use for our development (like xpl, FCF, coqhammer, and coqSMT).

After the right basis is selected we will start selecting sample programs and trying to prove things about them in Coq. At this point we will decide in which direction the project is going to continue.

## Provisional Table of Contents

- Abstract (10-20 lines)
- Section 1: Introduction (1-2 pages)
- Section 2: Theory and existing frameworks (4-8 pages)
- Section 3: Our approach (6-12 pages)
- Section 4: Our contribution (6-12 pages)
- Section 5: Comparison to other work and ideas for future work (2-4 pages)
- Section 6: Conclusion (1-2 pages)
- Acknowledgements (3-5 lines)
- References ($\frac{1}{2}$-1 page)
- Appendix with programming code, tables, full proofs, etc. (5-20 pages)

## Provisional Time Plan

**First week of February (15 hours)**
Planning of activities, including the production of the Bachelor's contract.

**Rest of February and first half of March ($3 \times 15$ hours)**
Read literature and research the current state of the art tools for formal cryptographic proofs; rough draft of Section 2 in Bachelor's report.

**Rest of March until start of May ($2 \times 15 + 8 \times 30$ hours)**
Work on the design and implementation of our contribution. Keep adding to the report along the way.

**End of May and first half of June ($3 \times 30$ hours)**
Write the missing parts, put drafts together, make things consistent, proof reading.