

UiO Master Thesis proposals, Fall 2021

Michael Kirkedal Thomsen

Associate Professor, PT (10th floor)

michakt@ifi.uio.no

Areas of interest

- Domain specific programming languages and computation models in general
- Information security and communication
- Decentral systems (information handling and consensus)
- Models for improved reliability; e.g. reversibility, probabilistic and quantum computations

Experienced supervisor

- I have supervised about 20 Master's Thesis and 50 Bachelor's projects.
- Several of these have resulted in research publications

Suggestions

The following suggestions is arranged from practical application towards basic research.

If you have your own suggestion for projects relating to the above or later suggests, I'm very interesting to hearing about it.

Secure Decentral Communication for the Maritime Sector

The maritime sector is in an interesting process of digitalised. That ranges from ship communication and route planning to autonomous ships, which add significant requirements to the security and reliability of these decentral systems.

This project will be about specifying and implementing protocols for secure and reliable decentral maritime communication. It will build on the identity systems of the Maritime Connectivity Platform (MCP) [1] and the development will be in close collaboration with international members of the consortium behind. The protocols will target communication protocols over both IP network and the VDES radio network.

For this project will build on knowledge of secure networking protocols (e.g. TLS, HTTPS and PGP) and reliability for decentralised systems. The target is to develop real works use cases and library software, that can be the foundation for later production software. Furthermore, it will be expected to provide knowledge and text for future standards in the area.

[1] Maritime Connectivity Platform: <https://maritimeconnectivity.net/>

Decentral Trust for the Maritime Sector

The maritime sector is in an interesting process of digitalised. That ranges from ship communication and route planning to autonomous ships, which add significant requirements to the security and reliability of these decentral systems.

Within the Maritime Connectivity Platform (MCP) [1] we are currently developing a the proof-of-concept for a maritime decentral trust system, that will be done over the fall. This is build on a MPC identity systems and a system from P3KI [2].

This project will continue this work towards an implementation based on real actors (governance from maritime organisations and companies). Further, it will develop a querying service for the decentral system, that provides a proof of the trust chain.

For this project will build on basic cryptographic principles and reliability for decentralised systems. The target is to develop real works use cases and library software, that can be the foundation for later production software. Furthermore, it will be expected to provide knowledge and text for future standards in the area.

[1] Maritime Connectivity Platform: <https://maritimeconnectivity.net/>

[2] P3KI: <https://p3ki.com/>

Hermes: Reversible language

A many attacks to encryption algorithms can today be linked to side-channels; that is unintended implementation or execution specific behaviour that "leaves" information behind that has the possibility to be used to break the encryption.

This project will investigate the usage of reversible programming as a way to increase resilience against side-channels. The will build on a preliminary investigation and include:

- * Reversible computations is a restricted computation model with possible applications to energy-efficient, secure and reliable (though information preservation) computations.
- * Model has applications to "real work" where the inherent properties can be exploited.

The project will specifically work on

- * Identify possible side-channels and their effects
- * Create testing framework that can profile for side-channels
- * Investigate existing reversible Janus implementations of light-weight encryption algorithms
- * (Partly) implement more advanced encryption algorithms
- * Consider the suitability of Janus as an implementation language

Reliable Concurrent Computations

In this thesis you will be designing the fundamentals of this concurrent (actor based, like Erlang) reversible programming language, focusing on the interaction between actors and how to model I/O. The computational part of this language will be assumed at this stage and could be done as calls (and uncalls) to existing reversible programming languages programs, allowing me to focus on the concurrent parts of the language.

I will also be creating a compiler to compile this language into equivalent non-reversible Erlang code, allowing for simulation on non-reversible hardware. Performance will not be an important factor for the compiler, as it serves merely as a proof of concept. Erlang is chosen as it is a robust functional, concurrent and distributed language that is used both within academia as well as in the industry.

Relationship between reversible and probabilistic computations

The idea is to investigate the functional models behind reversible and probabilistic computations models (lambda calculus) and development a unifying model.

This will have implications towards usage in achieving consensus reliable decentral systems.

This project is basic research, so talk to me about the details project.

Questions?