# Outline

## (Abstract)

## 1) Introduction

Primer on (c-) lightning, networking aspects (in particular gossiping and probing mechanisms), possible information which can be extracted, and how that information is useful.

## 2) Retrieving information via existing RPC calls

Exploring c-lightning's RPC interface with Python and seeing how much information I can gather with the default implementation of c-lightning. In addition, examining how that information can be pieced together to reveal potential security / privacy concerns.

## 3) Retrieving more information via altering c-lightning code

Expanding upon 2), the goal will be to explore how much further this can be taken by altering c-lightning code and running a custom-compiled implementation (more in a proof of concept manner rather than extensive testing / recoding).

## 4) Security implications

Discuss the tangible results of 3) and 4). Maybe illustrate found issues based on an example (testnet / regtest infrastructure). Possibly offer mitigation advice, if feasible.

## 5) Related work

Currently consisting of:

- https://arxiv.org/pdf/1902.05260.pdf

- https://arxiv.org/pdf/1909.06890.pdf
- https://arxiv.org/pdf/1902.07307.pdf
- https://arxiv.org/pdf/1901.04972.pdf

Point to resources which helped me kickstart my project.

## 6) Conclusion

Talk about other conclusions, which have not been discussed in 4). Summarize work, provide research outlook.

## 7) References