



AARHUS
UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE

BACHELOR THESIS

The robot attack something etc.

Author:

Marcus Sellebjerg

Student number:

201808635

Here is some text

March 12, 2021

Contents

- 1 Introduction
- 2 Oracle attacks
- 3 PKCS padding
- 4 Bleichenbachers attack from 1998
- 5 Why it's hard to remove the oracle
- 6 Different variations of the attack
- 7 Probable solutions
- 8 solutions implemented in danskebank / other places
- 9 Eventually solving it with ECC