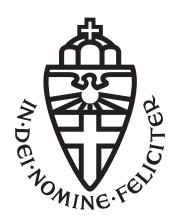
# BACHELOR THESIS



## RADBOUD HONOURS ACADEMY

### TBD

Author: Stijn Vandenput Supervisor: Martijn Stam Bart Mennink

20/05/2022

Bacholer Thesis Page i

## Abstract

not even sure if a bachelor thesis has a abstract test [1], [2]

Bacholer Thesis Page ii

## Contents

1	Introduction	1
2	Preliminaries	1
3	Existing AE/DEM notations in more detail	1
4	New Definition	1
5	Constructions	1
6	Use cases	1
7	Related Work	2
8	Conclusion	2
Re	Constructions Use cases Related Work Conclusion Ferences	
9	Appendix	3

Bacholer Thesis Page 1

#### 1 Introduction

should consist of:

- explaining the challenge
- my contribution

#### 2 Preliminaries

should consist of:

- recapping known definitions
- primitive definitions

## 3 Existing AE/DEM notations in more detail

should consist of:

• the def of the two paper, if possible already brought more toward one notation standard

#### 4 New Definition

should consist of:

- syntax of the primitive (input,output,correctness,tidiness)
- game based code
- explanation of the choices made
- formal comparison with other choices

#### 5 Constructions

should consist of:

- $\bullet$  how to construct the new primitive from old primitives
- security bounds
- comparison with existing alternatives

#### 6 Use cases

should consist of:

• possible use cases

Bacholer Thesis Page 2

## 7 Related Work

Location not final yet

## 8 Conclusion

Bacholer Thesis Page 3

## References

[1] C. Namprempre, P. Rogaway, and T. Shrimpton, "Reconsidering generic composition," 2014, pp. 257-274. DOI:  $10.1007/978-3-642-55220-5_15$ .

[2] C. Namprempre, P. Rogaway, and T. Shrimpton, Reconsidering generic composition, Cryptology ePrint Archive, Report 2014/206, https://eprint.iacr.org/2014/206, 2014.

## 9 Appendix

