

SPECIFICATION

Zero Knowledge circuit

for continuation-passing interpreter



March 3, 2022

Abstract

Contents

1	Introduction	2
2	Lurk	2
2.1	Expressions	2
2.2	Environment	2
2.3	Continuation	2
2.4	Store	2
3	Circuit	2
3.1	Overview	2
3.2	Gadgets	2
3.2.1	Macros	2
3.2.2	Constraints	2
3.2.3	Pointer	2
3.2.4	Data	2
3.2.5	Multicase	3
4	Final remarks	3
5	References	3

1 Introduction

The book [1]

2 Lurk

2.1 Overview

t, nil
if
lambda
let
letrec
quote
atom
cons, car, cdr
arithmetic operations
equality
current env

2.2 Expressions

2.3 Environment

2.4 Continuation

2.5 Store

3 Circuit

3.1 Overview

3.2 Gadgets

3.2.1 Macros

Boolean
Equality
Pick

3.2.2 Constraints

Arithmetic operations

Utils

3.2.3 Pointer

Tag

Hash

3.2.4 Data

allocate

reverse lookup

3.2.5 Multicase

case

multicase

optimization

4 Final remarks

5 References

References

- [1] Daniel P. Friedman and Mitchell Wand. *Essentials of Programming Languages, 3rd Edition*. The MIT Press, 3 edition, 2008.