

SPECIFICATION

---

# Zero Knowledge circuit

for continuation-passing interpreter

---



March 2, 2022



**Protocol  
Labs**

## Abstract

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Lurk</b>	<b>2</b>
2.1	Expressions . . . . .	2
2.2	Environment . . . . .	2
2.3	Continuation . . . . .	2
2.4	Store . . . . .	2
<b>3</b>	<b>Circuit</b>	<b>2</b>
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
<b>4</b>	<b>Final remarks</b>	<b>3</b>
<b>5</b>	<b>References</b>	<b>3</b>

# **1 Introduction**

The book [1]

## **2 Lurk**

### **2.1 Expressions**

### **2.2 Environment**

### **2.3 Continuation**

### **2.4 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.