Discrete Logarithm Circuits

Elliot Snow-Kropla
Kyriakidis Group

September 27, 2013

The most straightforward way to make an AQC circuit for a one-way function is to take advantage of the fact that out computations are reversible; thus we just make a circuit for computing the function going the easy way.

1 Introduction

2 Background

2.1 Classical Computing

2.2 Quantum Computing

2.3 Adiabatic Quantum Computing

3 Quantum Circuit Compilation

3.1 QSM Language

3.2 Quantum Circuit

3.3 Embedding

```
def modular_power(b, e, m):
  r = 1
  while e > 0:
    if (e % 2) == 1:
      r = (r * b) % m
    e = e >> 1
    b = (b * b) % m
  return r
```

References