Breaking the RSA with Reversible Multiplier Circuits

Gustavo Estrela de Matos 8536051

April 27, 2016

1 The Problem

1.1 How to Break RSA Security

1.2 Reversible Multiplier Circuits

1.3 Goal of this Project

1.4 Restrictions and Limitations

2 Solving the Problem

2.1 Solution Evaluation

2.1.1 Bit Entropy

2.2 Genetic Algorithm

2.2.1 Population Start

2.2.2 Crossover

2.2.3 Mutation

2.3 Fitness Function

2.4 Local Beam Search

2.4.1 Choosing Next Step

3 Results

3.1 Sample Run

3.2 Analysis

4 Conclusion

4.1 Lessons Learnt

4.2 Future Research