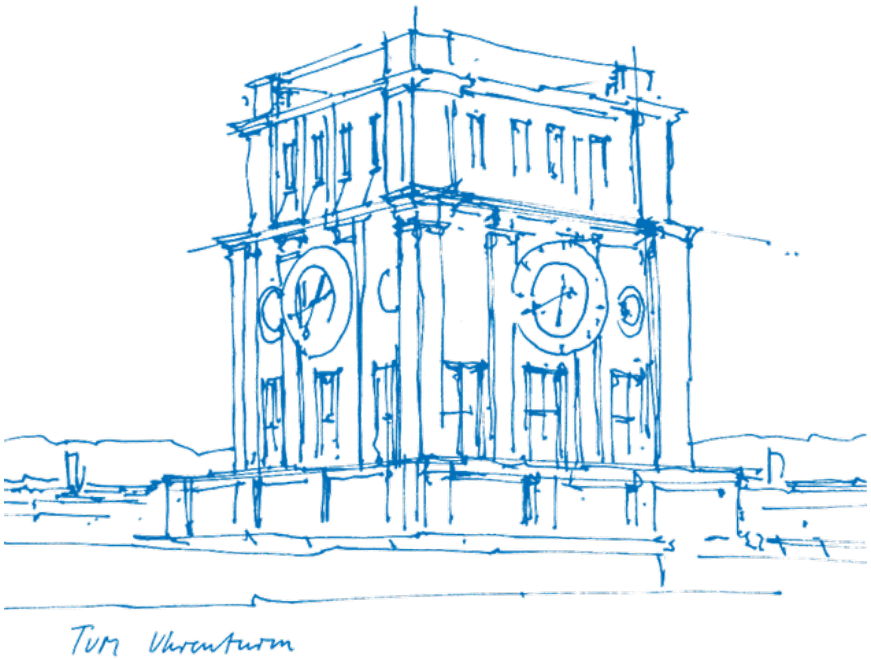
Chair for Security in Information Technology
School of Computation, Information and Technology
Technical University of Munich

Towards Efficient Helper Data Algorithms for Multi-Bit PUF Quantization

Marius Drechsler



Chair for Security in Information Technology
School of Computation, Information and Technology
Technical University of Munich

Towards Efficient Helper Data Algorithms for Multi-Bit PUF Quantization

Marius Drechsler

Thesis for the attainment of the academic degree

Bachelor of Science (B.Sc.)

at the School of Computation, Information and Technology of the Technical University of Munich.

Examiner:
Prof. Dr. Georg Sigl

Supervisor:
M.Sc. Jonas Ruchti

Submitted:
Munich, 22.07.2024

Contents

1 Introduction

These are the introducing words

1.1 Notation

To ensure a consistent notation of functions and ideas, we will now introduce some required conventions

Random distributed variables will be notated with a capital letter, i.e. X, its realization will be the corresponding lower case letter, x.

Vectors will be written in bold test: $\boldsymbol{k}$ represents a vector of quantized symbols.

We will call a quantized symbol k. k consists of all possible binary symbols, i.e. $0, 01, 110$.

A quantizer will be defined as a function $\mathcal{Q}(x, \boldsymbol{a})$ that returns a quantized symbol k.

Figure 1 shows the curve of a 2-bit quantizer that receives $\tilde{x}$ as input. In the case, that the value of $\tilde{x}$ equals one of the four bounds, the quantized value is chosen randomly from the relevant bins.

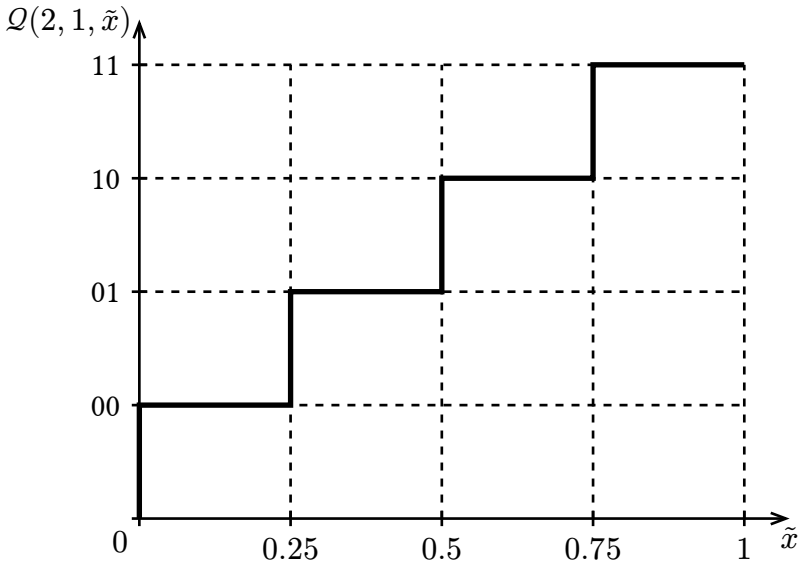


Figure 1: Example quantizer function

For the S-Metric Helper Data Method, we introduce a function

$$\mathcal{Q}(s, m) \tag{1}$$

where s determines the amount of metrics and m the bit width of the symbols.

Babla from Equation 1

2 Background

2.1 Quantum Computation and Quantum Circuits

A quantum computer is a device that performs calculations by using certain phenomena of quantum mechanics. The algorithms that run on this device are specified in quantum circuits.

Example

Figure 2 shows a simple quantum circuit that implements a specific quantum algorithm.

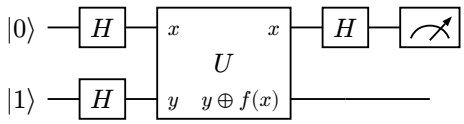


Figure 2: A quantum circuit implementing the Deutsch-Jozsa algorithm

2.2 Decision Diagrams

Decision diagrams in general are directed acyclical graphs, that may be used to express control flow through a series of conditions. It consists of a set of decision nodes and terminal nodes. The decision nodes represent an arbitrary decision based on an input value and may thus have any number of outgoing edges. The terminal nodes represent output values and may not have outgoing edges.

A binary decision diagram (BDD) is a specific kind of decision diagram, where there are two terminal nodes (0 and 1) and each decision node has two outgoing edges, depending solely on a single bit of an input value. BDDs may be used to represent any boolean function.

Example

Example BDDs implementing boolean functions with an arity of 2 are show in Figure 3 and Figure 4.

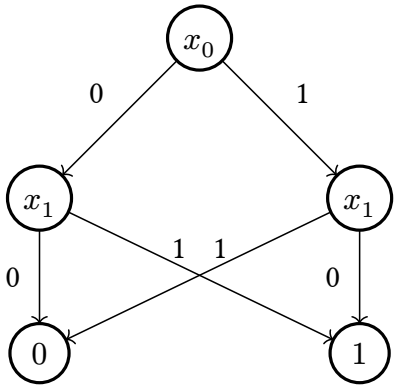


Figure 3: A BDD for an XOR gate.

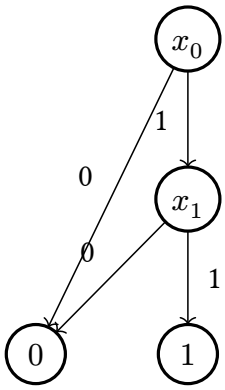
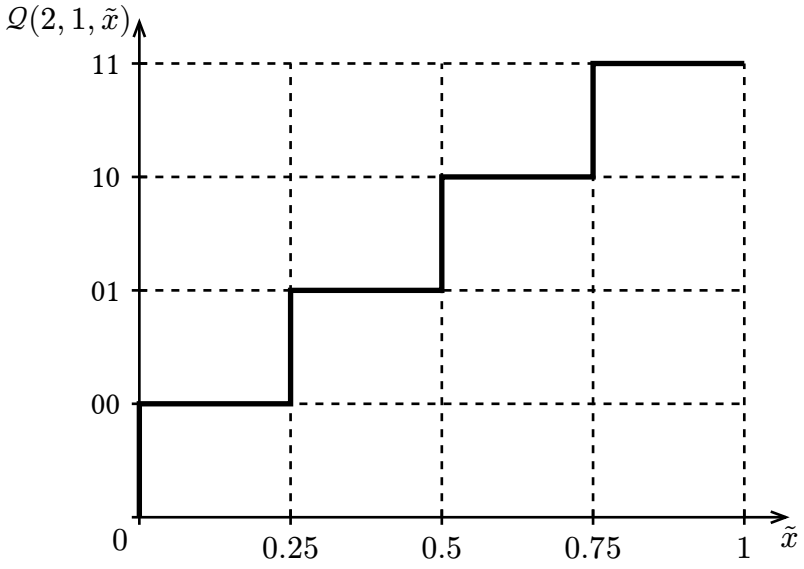


Figure 4: A BDD for an AND gate.

3 S-Metric Helper Data Method



4 State of the Art

There are a variety of existing approaches to providing a suitable oracle for quantum circuit equivalence checking based on decision diagram (DDs). Quantum Circuit Equivalence Checker (QCEC) currently implements gate-cost, lookahead, one-to-one, proportional and sequential application schemes. (Burgholzer and Wille)

5 Implementation

5.1 Visualisation

Initially, a visualisation of the diff algorithms applied to quantum circuits was created to assess their usefulness in equivalence checking. Additionally, this served as exercise to better understand the algorithms to be used for the implementation in QCEC.

5.2 QCEC Application Scheme

The Myers' Algorithm was implemented as an application scheme in QCEC.

```
do something
do something else
while still something to do
    do even more
    if not done yet then
        wait a bit
        resume working
    else
        go home
    end
end
```

Figure 6: Myers' algorithm.

5.3 QCEC Benchmarking Tool

As QCEC doesn't have built-in benchmarks, a benchmarking tool was developed to test different configurations on various circuit pairs.

6 Benchmarks

6.1 Google Benchmark

6.2 MQT QCEC Bench

To generate test cases for the application schemes, Munich Quantum Toolkit (MQT) Bench was used. (Quetschlich et al.)

Benchmark Name	**Diff Run Time**	**Proportional Run Time**
DJ	$1.2 \cdot 10^{-6}\,\mathrm{s}$	$1.5 \cdot 10^{-6}\,\mathrm{s}$
Grover	$1.3 \cdot 10^{-3}\,\mathrm{s}$	$1.7 \cdot 10^{-3}\,\mathrm{s}$

7 Conclusion

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius. Ego autem mirari satis non queo unde hoc sit tam insolens domesticarum rerum fastidium. Non est omnino hic docendi locus; sed ita prorsus existimo, neque eum Torquatum, qui hoc primus cognomen invenerit, aut torquem illum hosti detraxisse, ut aliquam ex eo est consecutus? – Laudem et caritatem, quae sunt vitae.

8 Outlook

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius. Ego autem mirari satis non queo unde hoc sit tam insolens domesticarum rerum fastidium. Non est omnino hic docendi locus; sed ita prorsus existimo, neque eum Torquatum, qui hoc primus cognomen invenerit, aut torquem illum hosti detraxisse, ut aliquam ex eo est consecutus? – Laudem et caritatem, quae sunt vitae.

Glossary

***BDD* – binary decision diagram**. 8, 9

***DD* – decision diagram**. 11

***MQT* – Munich Quantum Toolkit**. 13

***QCEC* – Quantum Circuit Equivalence Checker**. 11, 12

Bibliography

Burgholzer, Lukas, and Robert Wille. “Advanced Equivalence Checking for Quantum Circuits.” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 9, Sept. 2021, pp. 1810–24, https://doi.org/10.1109/tcad.2020.3032630

Quetschlich, Nils, et al. “MQT Bench: Benchmarking Software and Design Automation Tools for Quantum Computing.” *Quantum*, 2023