

Jacob Herbst (mwr148), Jonas Flach Jensen ()

Crypto in SME for FPGA

Advisor: Kenneth Skovhede

February 24, 2021

Contents

1	Introduction	3
2	Background	3
2.1	FPGA	3
2.2	SME and CSP	3
2.3	A crypto library	3
2.3.1	Hashing	3
2.3.2	MD5	3
3	Implementation	3
3.1	Approaches	3
3.1.1	naive	3
3.1.2	pipelined	3
3.2	MD5	3
3.2.1	naive	3
3.2.2	pipeline 1	3
4	Benchmarks	3
5	Discussion	3
6	Conclusion	3

1 Introduction

2 Background

2.1 FPGA

2.2 SME and CSP

2.3 A crypto library

2.3.1 Hashing

2.3.2 MD5

3 Implementation

3.1 Approaches

3.1.1 naive

3.1.2 pipelined

3.2 MD5

3.2.1 naive

3.2.2 pipeline 1

4 Benchmarks

5 Discussion

6 Conclusion

References

....