Constant-Time Big Numbers (for Go)

Lúcás Críostóir Meier

School of Computer and Communication Sciences

Decentralized and Distributed Systems lab (DEDIS)

BSc Semester Project

May 2021

Responsible and Supervisor
Prof. Bryan Ford
EPFL / DEDIS

Contents

1 Introduction

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vestibulum a erat non augue vulputate aliquam. Nullam non felis id velit convallis dapibus eu quis risus. Nulla egestas, erat vel hendrerit sagittis, erat urna viverra libero, id ornare massa mauris ac quam. Sed tincidunt pretium lacus, eu hendrerit velit laoreet ut. Morbi mattis vestibulum leo eget imperdiet. Donec id condimentum magna. Nulla cursus facilisis erat. Sed id nulla non tortor venenatis blandit eget sed metus. Vivamus mollis mollis nulla, eu mattis neque tristique a. Nunc risus metus, pharetra nec mollis nec, lacinia vel enim. Cras ut felis nunc. Curabitur felis felis, lobortis in elementum quis, adipiscing in velit.

Sed lectus arcu, consequat eu interdum quis, suscipit nec risus. Fusce magna elit, pretium vel pulvinar sed, pulvinar et leo. Nunc non orci et lacus luctus aliquam eu ac augue. Nunc gravida lectus vitae tortor posuere rhoncus. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis nec diam orci. Praesent nisl dui, fringilla sodales blandit et, bibendum et leo. Nullam molestie, erat nec ultrices tincidunt, eros quam ornare sem, in egestas orci turpis at risus.

Sed lectus arcu, consequat eu interdum quis, suscipit nec risus. Fusce magna elit, pretium vel pulvinar sed, pulvinar et leo. Nunc non orci et lacus luctus aliquam eu ac augue. Nunc gravida lectus vitae tortor posuere rhoncus. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis nec diam orci. Praesent nisl dui, fringilla sodales blandit et, bibendum et leo. Nullam molestie, erat nec ultrices tincidunt, eros quam ornare sem, in egestas orci turpis at risus.

Sed lectus arcu, consequat eu interdum quis, suscipit nec risus. Fusce magna elit, pretium vel pulvinar sed, pulvinar et leo. Nunc non orci et lacus luctus aliquam eu ac augue. Nunc gravida lectus vitae tortor posuere rhoncus. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis nec diam orci. Praesent nisl dui, fringilla sodales blandit et, bibendum et leo. Nullam molestie, erat nec ultrices tincidunt, eros quam ornare sem, in egestas orci turpis at risus.

See: [Koc96]

2 Background

2.1 Big Numbers in Cryptography

2.2 Side-Channels

2.2.1 Our Threat-Model

2.2.2 Vulnerabilities in `big.Int`

3 Implementation

3.1 The `safenum` library

3.1.1 Handling Size

3.2 Some Basic Techniques

3.3 Some Algorithm Choices

4 Results

4.1 Comparison with `big.Int`

4.2 Comparison with `go/crypto`

5 Further Work

5.1 Upstreaming to `go/crypto`

6 Conclusion

References

[Koc96] Paul C Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. page 10, 1996.