
# Introduction To Linear Cryptanalysis

Maximilian Heim

# Contents

**1 Abstract** **2**

**2 Introduction** **2**

**3 Impact** **2**

**4 Theory** **2**

**5 Demonstration** **2**

**6 Protection** **2**

**7 Conclusion** **2**

**8 References** **2**

**9 Appendix** **2**

# 1 Abstract

# 2 Introduction

**Cryptanalysis** Cryptanaylsis is the process of extracting secret cryptographic keys from plaintext/ciphertext pairs. Several attack vectors have been found to generally be applicable to certain algorithms, apart from that there is a lot of research going on to refine (and hopefully prevent) these attacks. In terms of modern standards most of these attacks aren't applicable to the cryptographic algorithms with their corresponding keysize, though everywhere old systems are still in use. It's important to explore all the possibilities to make the systems that replace the old ones safer.

**About** In this paper we will explore linear cryptanalysis which is one of the main two branches of cryptanalysis that exist. The other being differential cryptanalysis. We will explore the impact of such attacks on finance and algorithm design. Apart from that how to create such an attack, give a demonstration of it and show how to protect a cryptographic system from it.

# 3 Impact

# 4 Theory

# 5 Demonstration

# 6 Protection

# 7 Conclusion

# 8 References

# 9 Appendix