

Romulus Beyond Benchmarking

Investigating the Capabilities outside of Dogmatic Benchmarking Frameworks

Mustafa Khairallah

February 2, 2022

1 Introduction

Romulus [1] is a family of lightweight cryptographic schemes. It includes 3 Authenticated Encryption with Associated Data (AEAD) schemes and a hash function. Rom