Hermes
Building a practical multi-device SPARTA

Surendra Jammishetti
CSE 108C
sjammish@ucsc.edu

I. Introduction

With the threat of a global adversary looming over online communication, its becoming a more pressing concern to have secure, relaible, messaging services. We came up with E2E encryption to protect the contents of our messages, but its not enough to protect against a global adversary. E2E encryption doesnt hide the metadata of our conversations, as the adversary can still reconstruct who is talking to who, and when. The SPARTA construction offers a metadata-private anonymous communication system, and for the first part of my project it'll detail the implementation of SPARTA-LL. After initially reading the Groove paper, which has support for users to have multiple devices via a untrusted provider, it inspired me to try incorporating similar functionality into my project. Additionally I've been able to get my SPARTA implementation running inside an AWS Nitro Enclave!

II. Base Sparta

A. *Facebook PathORAM discussion*

III. Multi-Device Extension

IV. Experiments and Results

V. Conclusion

References