

Pomona College
Department of Computer Science

Decentralized Group Management in Dissent

Eleanor Cawthon

April 25, 2015

Submitted as part of the senior exercise for the degree of
Bachelor of Arts in Computer Science
Professors Bryan Ford and Tzy-Yi Chen, advisors

Copyright © 2015 Eleanor Cawthon

The author grants Pomona College the nonexclusive right to make this work available for noncommercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.

Abstract

Decentralized approaches to private communication exhibit tradeoffs between decentralization and scalability. We present a protocol for achieving the best of both worlds.

added to make it compile, this abstract is not a draft

Contents

Abstract	i
List of Figures	v
List of Tables	vii
Preface	ix
1 Background and Related Work	1
2 Goals and Non-Goals	3
3 Protocol Description	5
4 Security Properties and Correctness	7
5 Evaluation	9
6 Conclusion	11

List of Figures

List of Tables

Preface

Chapter 1

Background and Related Work

Chapter 2

Goals and Non-Goals

Chapter 3

Protocol Description

Chapter 4

Security Properties and Correctness

Chapter 5

Evaluation

Chapter 6

Conclusion