El Gamal Mix-Nets and implementation of a verifier

Carl Svensson & Erik Larsson

March 6, 2013

Contents

1 Introduction **2**

2 El-Gamal cryptography **2**

3 Mix-Nets **2**
3.1 Verifier 2

4 Specification docs **2**

5 Implementation of the verifier **2**
5.1 General design choices 2
5.2 Third party libraries 2
5.3 Math library 2
5.4 PRGs and ROs 2
5.5 Verifier 2
5.6 Tests 2
5.7 Performance 2

6 Conclusions **2**

7 References **2**

1 Introduction

2 El-Gamal cryptography

3 Mix-Nets

3.1 Verifier

4 Specification docs

5 Implementation of the verifier

5.1 General design choices

5.2 Third party libraries

5.3 Math library

5.4 PRGs and ROs

5.5 Verifier

5.6 Tests

5.7 Performance

6 Conclusions

7 References