

El Gamal Mixnets and Implementation of a  
Verifier  
SA104x Degree Project in Engineering Physics  
KTH Royal Institute of Technology  
School of Computer Science and Communication  
Supervisor: Douglas Wikström

Carl Svensson carlsven@kth.se & Erik Larsson erikl3@kth.se

April 11, 2013

**Contents**

# 1 Introduction

Why cryptography?

Classical vs Modern cryptography

Public key cryptosystem

Uses (Communication, Signatures?, Verification)

Mix networks

Verificatum Mixnet

Verification and its importance

Implementation

# 2 El Gamal Cryptography

## 2.1 Definition

The El-Gamal cryptosystem is defined over a group  $G_q = \langle g \rangle$  of prime order  $q$ , generated by  $g \in G_q$ . A private key  $x \in \mathbb{Z}_q$  is chosen randomly and is used to compute the public key  $(g, y) \in G_q \times G_q$  where  $y = g^x$ .

Encryption of a plaintext  $m \in G_q$  is done by choosing a random  $s \in \mathbb{Z}_q$  and computing  $(u, v) \in G_q \times G_q$  where  $u = g^s$  and  $v = y^s m$ . Decryption of a ciphertext  $(u, v) \in G_q \times G_q$  is achieved by using the private key  $x$  to compute  $m = u^{-x} v$ .

## 2.2 Security

Let  $b = g^a \in G_q$  where  $a \in \mathbb{Z}_q$ . Then  $a$  is said to be the discrete logarithm of  $b$  in the group  $G_q$ . There is currently no known efficient classical algorithm that given  $(G_q, g, b)$  is able to calculate  $a$  in a reasonable amount of time (polynomial time). The discrete logarithm problem is thus considered to be a hard problem. (Källa)

The security of the El Gamal cryptosystem relies on the difficulty of discrete logarithm in finite cyclic groups  $G_q$ . This means that the El Gamal cryptosystem is secure as long as no one is able to compute the discrete logarithm in  $G_q$  efficiently. (Källa)

## 2.3 Properties

The El Gamal cryptosystem is a homomorphic cryptosystem. This

Generalization

## 3 Cryptographic Primitives

PRGs ROs

## 4 Mix Networks

### 4.1 Overview

Intuitiv beskrivning (gör bättre)

<http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/universal/Universal.pdf>

One purpose of mix networks, or mixnets, is to provide untraceability to its users. A mixnet may, for example, take as input a list of encrypted messages of different origins. These messages pass through the mixnet and is output decrypted and in a randomized order. This property may be used to enable anonymous voting systems.

A reencryption mixnet consists of a number of servers which sequentially process the messages and reencrypts the list of messages and outputs them in a randomized order. After passing through all servers, the list of ciphertexts is decrypted and the result is a list of the messages in random order. It is impossible to deduce from where each element came.

### 4.2 El Gamal Mixnets

### 4.3 Operation

### 4.4 Verification

## 5 Specification/Documentation

Vilken dokumentation har vi använt oss av?

## **6 Implementation of the Verifier**

### **6.1 General Design Choices**

Programming language?

Objects, UML

### **6.2 Third Party Libraries**

#### **6.2.1 Arithmetic Library**

GMP why?

#### **6.2.2 XML Parser**

RapidXML why?

#### **6.2.3 Cryptographic Primitives**

OpenSSL why?

#### **6.2.4 Testing**

Google Test why?

### **6.3 Math Library**

Hur och varför har vi gjort som vi gjort?

### **6.4 Pseudorandom Generators and Random Oracles**

### **6.5 Verifier**

### **6.6 Tests**

### **6.7 Performance**

Viktigt?

## **7 Conclusion**

Kunde dokumentationen ha gjorts bättre?

## **8 References**