Polycyclic Group Based Cryptography and Implementation

Yoongbok Lee

College of William and Mary
Department of Mathematics

Honors Thesis 2017-2018

1. Introduction to Cryptography
   - Public-key Cryptography
   - Vulnerability
2. Introduction to Groups
   - Finitely Presented Group
3. Group Based Cryptography
   - Examples of Group Based Cryptography
   - Some Algorithmic Problems for Proper Platform Groups
4. My research

Cryptography

- Definition
  - The art of encoding and decoding messages
- Public-key
  - A cryptography based on a publicly known key and a secret private key

Public-key Cryptography

Vulnerability

- Relies on the hardness of decomposing composite numbers
- the size of keys has to grow to avoid possible brute-force attacks

Group

- A group G is a collection of elements that satisfy these properties :
  - identity
    $\exists e \in G$ such that $g * e = e * g = g$ for all $g \in G$
  - inverse
    $\forall g \in G, \exists h$ such that $g * h = h * g = e$.
    We write $h = g^{-1}$
  - associativity
    $\forall a, b, c \in G, (a * b) * c = a * (b * c)$

Finitely Presented Group

- Group given by its generators and relations
- General Form
  - $G = \langle x_1, x_2, \cdots | r_1, r_2, \cdots \rangle$
    where each r_i's represent the identity of the group

Group Based Cryptography

Cryptosystem based on various kinds of groups (including the group of integers)

Examples of Group Based Cryptography

- Diffie-Hellman protocol
- Anshel-Anshel-Goldfeld protocol
- ElGamal protocol

Some Algorithmic Problems for Platform Groups

- decision and search problems
  - word problem
    Given a word $g \in G$, decide whether $g = e$ in G.
  - membership problem
    Given a word $g \in G$ and a subgroup $H \leqslant G$, decide whether $g \in H$
  - conjugacy problem
    Given elements $g, h \in G$, decide if $g = x^{-1}hx$ for some $x \in G$
  - $\cdots$

Diffie-Hellman Based Semigroup Cryptosystem