Polycyclic Group Based Cryptography and Implementation

Yoongbok Lee

College of William and Mary
Department of Mathematics

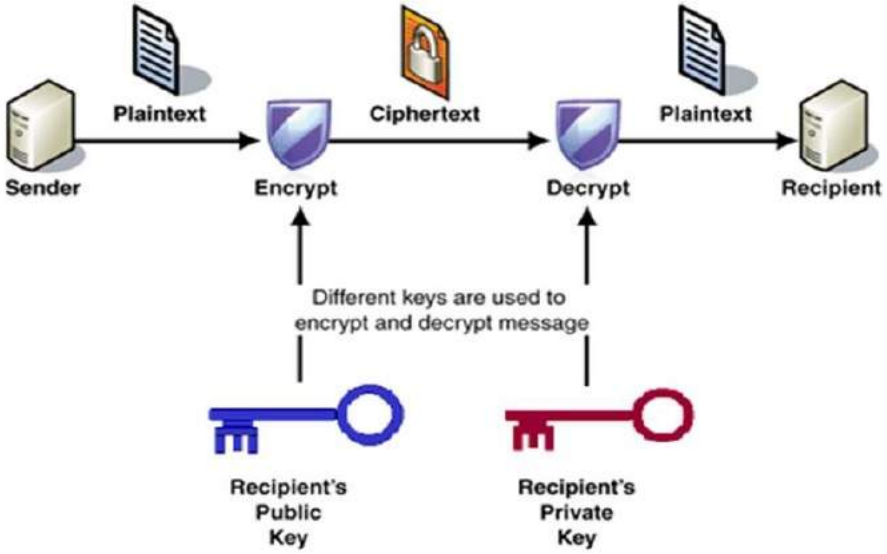
Honors Thesis 2017-2018

1. Introduction to Cryptography
   - Public-key Cryptography
   - Vulnerability
2. Introduction to Groups
   - Finitely Presented Group
3. Group Based Cryptography
   - Examples of Group Based Cryptography
4. My research
   - Ko-Lee protocol & Nonlinear Decomposition Attack
   - implementation and efficiency analysis

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 Cryptogrpahy



Diffie-Hellman

- Example: Diffie-Hellman protocol
  - In some set G
  - Alice and Bob's private key a and b, respectively.
  - For a known element $g \in G$, Alice and Bob's keys: g^a and g^b, respectively.
  - Shared secret key: $(g^a)^b = (g^b)^a = g^{ab}$

Vulnerability

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

Group

- A group G is a collection of elements under a binary operation (*) that satisfies 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
    $\forall a, b, c \in G, (a * b) * c = a * (b * c)$
- Note: A group does not have to be commutative!
  $(ab \neq ba)$

Finitely Presented Group

- Group given by its generators and relations
- $G = \langle x_1, x_2, \cdots | r_1, r_2, \cdots \rangle$
  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 under addition)

Examples of Group Based Cryptography

- Diffie-Hellman protocol
  - ElGamal protocol
- Anshel-Anshel-Goldfeld protocol
- Ko-Lee protocol

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 $x \in G$
  - ...

Diffie-Hellman Based Cryptosystem

- Given: Group G, A, B where $A, B \subseteq G$, $ab = ba (a \in A, b \in B)$, and $g \in G$
- Alice's key : g^a, Bob's key : g^b
- Shared key $= g^{ab} = g^{ba}$, can be obtained by both sides efficiently.

Nonlinear Decomposition Attack

- Main Idea: decomposing an element in a pre-determined set of elements
- works only if the membership search problem is efficiently solvable
- applicable to many other Diffie-Hellman scheme protocols

implementation and efficiency analysis

- Goal
  - Build a functional model of the attack
  - analyze the complexity of the model
- GAP
  - provides various built-in functions related to Abstract Algebra
  - package "Polycyclic"
- Current status
  - Implementation complete, working as intended
  - Implement in different platform groups and protocols

Implementation

- Decryption
  - find generating set of g^A in terms of g^a's, $a \in A$.
  - solve Alice's public key (g^a) in terms of those generating set
  - compute g^{ab}

Testing the Implementation

Average time in milliseconds of 100 trials $|G| = 2 \times p^6$

	Alice and Bob	Eve
5	~ 0	15.92
7	~ 0	38.56
11	~ 0	719.44
13	~ 0	5112.64
17	~ 0	11982.76
19	~ 0	23941.04
21	$\sim 1/4$	113164.88