Midterm Report: Cryptography using finite, non-abelian groups

Emile Doering

Project Advisor: Dr. Aaron Wootton

Fall 2004
University of Arizona
The current project is to study, understand and implement on a small scale the results of a paper by Magliveras, Stinson and Trung entitled “New Approaches to designing public-key cryptosystems using one-way functions and trap-doors in finite groups”. The focus of their paper is on developing not only a new cryptosystem but an entirely new type of cryptosystem. What follows is an outline of information gained in our study thusfar.

Most of the currently unbroken public-key cryptosystems have their basis in relative difficulty (not impossibility) of solving certain problems or certain types of problems in an abelian group. Examples include: multiplicative groups of units in a ring of integers mod $pq$ with $p$ and $q$ primes, or multiplicative groups in some finite field. The proposed new approach promises public keys, the solutions to which are genuinely unsolvable, through the use of permutation groups rather than rings or fields as bases for the system. These groups are not cyclic (have no generating element) and have far greater complexity than any cyclic group of similar size.

In thoroughly developing the ideas in the cited paper, the first step is to become acquainted with numerous definitions, many of which will be skipped in this outline or only referred to as needed. One definition that is central to the project and cannot be skipped is that of a logarithmic signature. If $G$ is a finite group, and $G^Z$ is the set of all finite sequences in $G$, then a convenient visualization of a pair of these sequences is as a pair of row (or column) matrices,

$$[a_1, a_2] \circ [b_1, b_2, b_3] = [a_1 b_1, a_1 b_2, a_1 b_3, a_2 b_1, a_2 b_2, a_2 b_3]$$
where \( \circ \) is the tensor product between sequences \( A \) and \( B \) in \( G^2 \). A logarithmic signature (denoted \( \alpha \)) for the group \( G \) is a finite product of sequences of \( G^2 \) such that every element of \( G \) is present once and only once in the resultant sequence.

An important fact that follows from the definition of the logarithmic signature is that if \( \alpha = [A_1, A_2, \ldots, A_n] \) is a logarithmic signature for \( G \) then every element of \( G \) has a unique factorization of \( p_i \) in \( A_i \).

A few more definitions are needed; the **length** of \( G \) is its number of elements \( (L) \) and the **degree** of \( G \) is defined to be the least integer \( n \) such that \( \log(L) \leq \lceil n \log(n) \rceil \), \( \log(n) \) rounded down to an integer. If the factorization of \( p_i \) in \( A_i \) can be achieved in polynomial time then we say that the logarithmic signature is *tame*. If this factorization can be achieved in time bounded by a polynomial in \( n^2 \), then the logarithmic signature \( \alpha \) is *supertame*. If \( \alpha \) is not tame, it is *wild*.

A very important observation on logarithmic signatures is that since they contain every element of \( G \) exactly once, their existence implies the existence of a surjection \( \hat{\alpha}: S \rightarrow G \) from a set \( S = \{0 \leq k \leq L\} \) of positive integers to \( G \). By defining an order relation on the elements of \( G \) (the exact means of defining this is not important, so long as the relation is defined on all of \( G \)), it is also possible to define \( \hat{\alpha}^{-1}: G \rightarrow S \), and we then have a bijection. Then \( \hat{\alpha} \) is an invertible function, and as is proved in the paper, it is always computable. However, its *inverse* is computable if and only if \( \alpha \) is tame.

This leads us to one of the most important results of the paper: If \( \hat{\eta} \) is a tame logarithmic signature for \( G \) and \( \hat{\alpha} \) is a wild logarithmic signature, then \( \hat{\alpha} \hat{\eta}^{-1}: G \rightarrow S \) is a one-way permutation on \( S \). It is extremely important to note that the existence of wild logarithmic signatures has not been confirmed. The most that has yet been shown is that
some logarithmic signatures exhibit “wild-like” behavior. This is an area of ongoing research in group theory.

Nevertheless, the possible uses of wild logarithmic signatures takes on an obvious relevance in the context of cryptosystem construction; the builder of any cryptosystem wants a key that is easy to decode one way, but very difficult to decode going the other way. If wild logarithmic signatures exist, they would provide the means to construct an unbreakable public key.

The plan for the remaining portion of the project is as follows: First, to develop the idea of equivalence classes of logarithmic signatures. Having a clear criterion for equivalence among logarithmic signatures will help minimize the chances that we will attempt to work with one that is “the same” as some other, tame logarithmic signature. As has been shown, the value of the idea of logarithmic signatures lies mainly in usage of the wild variety. We shall see that the only way to define a wild logarithmic signature is negatively, as one which is not tame and is in fact as un-tame as possible. Defining equivalence among tame signatures and among wild signatures then turns out to be the same endeavor.

Next we will study the brief outline given by Magliveras, et al. In their paper of a possible design for a new cryptosystem. The great question which will determine whether this approach will work in the long term is the question of whether wild logarithmic signatures for finite groups exist. Unfortunately, this question is beyond our means but we can and will study how such a system would work, and we can use logarithmic signatures which are “nearly” wild. This will be our approach in
implementing some of the suggestions of the paper and in building a small-scale version of one of their theoretic systems called MST 1.