1072-20-103 **David Garber*** (garber@hit.ac.il), 52 Golomb st., P.O.Box 305, 58102 Holon, Israel, and **Arkadius Kalka**, **Boaz Tsaban** and **Gary Vinokur**. *Super Summit Sets for the Multiple Conjugacy Problem in braid groups.* Preliminary report.

Let $v = (a_1, \ldots, a_n), w = (b_1, \ldots, b_n)$ be n-tuples of braids. The Multiple Conjugacy Problem (MCP) is that of deciding whether there is a braid x such that for each $i = 1, \ldots, n$, $xa_ix^{-1} = b_i$.

Lee and Lee (2002) defined a finite invariant subset of the cojugacy class of such vectors v, and proposed an algorithm for computing it, thus finding a finite time solution to the MCP. Gonzalez-Meneses (2005) presented a substantial improvement of this algorithm, but the invariant set is still too large. In the single conjugacy problem case, Lee-Lee's invariant set is larger than Garside's Summit Sets, and much larger than El-Rifai and Morton's (1994) Super Summit Set (SSS).

We introduce a much smaller invariant set, the Multiple Super Summit Set (MSSS), which is exactly the SSS in the single conjugacy problem case. The size of our MSSS tends to be a small constant, when n is just a constant multiple of the braid index. We supply an efficient way to compute the MSSS, using a generalization of Meneses's method of minimal elements. Our methods generalize to Garside groups as well.

The MSSS yields an efficient cryptanalysis of the Ko et al. cryptosystem (2000). We are considering its potential applicability to Shpilrain-Ushakov's cryptosystem (2006). (Received June 23, 2011)