1106-20-1069 **Lisa Bromberg** and **Vladimir Shpilrain***, shpil@groups.sci.ccny.cuny.edu, and **Alina Vdovina**. *Navigating the Cayley graph of $SL_2(F_p)$ and applications to hashing.*

Hashing with matrices refers to a simple idea of using a pair of matrices, A and B, to hash the 0 and 1 bit, respectively, and then to hash an arbitrary bit string in the natural way, by using multiplication of matrices. Since there are many known pairs of 2×2 matrices over Z that generate a free monoid, this yields numerous pairs of matrices over F_p, for sufficiently large primes p, that are candidates for collision-resistant hashing. However, this trick can "backfire", and lifting matrix entries to Z may facilitate finding a collision. This "lifting attack" was successfully used by Tillich and Zémor in the special case where two matrices A and B generate (as a monoid) the whole $SL_2(Z)$. However, we show that the situation with other, "similar", pairs of matrices from $SL_2(Z)$ is different, and the "lifting attack" can (in some cases) produce collisions in the *group* generated by A and B, but not in the positive *monoid*. Therefore, we argue that for these pairs of matrices, there are no known attacks at this time that would affect security of the corresponding hash functions. We also give explicit lower bounds on the length of collisions for hash functions corresponding to some particular pairs of matrices from $SL_2(F_p)$. (Received September 10, 2014)