1129-20-241 **Vladimir Shpilrain** (shpil@groups.sci.ccny.cuny.edu), City College of New York, NY , and **Bianca Sosnovski*** (bsosnovski@qcc.cuny.edu), Queensborough Community College, NY.

Semigroups of linear functions applied to Cayley hash functions.

Cayley hash functions are based on the idea of using a pair of elements in a (semi)group, A and B, to hash the 0 and 1 bit, respectively. A bit string is associated to a string of A's and B's and the hash value is computed by multiplying the sequence of A's and B's in the (semi)group.

We present a new semigroup platform for a Cayley hash function. Our proposed hash function uses a pair of two linear functions in one variable over $\mathbb{F}_p$ under composition operation. The semigroup is generated by the functions $f(x) = 2x+1$ and $g(x) = 3x + 1$ modulo a prime $p > 3$. The result is an efficient hash function whose outputs are of size $2 \log p$. We give explicit lower bound on the length of collisions for the proposed hash function. (Received March 20, 2017)