1011-20-48 **Jean-Camille Birget*** (birget@camden.rutgers.edu), Dept. of Computer Science, Rutgers University at Camden, Camden, NJ 08102. *Algebraic characterizations of one-way functions.* Preliminary report.

One-way functions are a fundamental concept of cryptography. They are functions between words over a finite alphabet such that it is "easy" to compute $f(x)$ on input x, but given y it is "extremely hard" to find any x such that $f(x) = y$. When f is a function between bit-strings of length n, we define "easy" to mean that f has a "small" acyclic digital circuit, and "extremely hard" to mean that all generalized inverses of f only have "very large" acyclic circuits. For all known reasonable definitions, it is an open problem whether one-way functions exist; the problem is related to P vs. NP.

We show that one-way permutations (between bit-strings of length n) exist if and only if the symmetric group $\mathfrak{S}_N$ (where $N = 2^n$) has super-polynomial distortion as a subgroup of the symmetric monoid F_N, as a function of n. The generating sets here consist of fixed finite sets, together with the transpositions of bit positions. Instead of the infinite family $\mathfrak{S}_N$ one can also use the Richard Thompson group V and the analogous monoid, and one can refine the result to finite generating sets. (Received August 03, 2005)