1020-11-257 **George B Purdy*** (george.purdy@uc.edu), ML 30, University of Cincinnati, Cincinnati, OH 45221-0030. *A Cryptographic Hash Function Based on Elliptic Curves.* Preliminary report.

A hash function is a function $f : X \rightarrow Y$ such that $|X| \geq 2|Y|$. We say that $f(x)$ is strongly collision-free if it is computationally infeasible to find x and x' such that $f(x) = f(x')$. We construct a hash function for a class of elliptic curves and prove that it is strongly collision-free relative to the discrete logarithm problem for elliptic curves. (Received August 29, 2006)