1106-VQ-2665 **Shyam S. Narayanan*** (shyam.s.narayanan@gmail.com), 8209 W 143rd Ter, Overland Park, KS 66223. *Improving the Speed and Accuracy of the Miller-Rabin Primality Test.* Preliminary report.

Currently, even the fastest deterministic primality tests run too slowly, with the Agrawal-Kayal-Saxena (AKS) primality test runtime $\tilde{O}(\log^6(n))$, and probabilistic primality tests are still highly inaccurate. In this paper, we discuss the accuracy of the Miller-Rabin Primality Test and the number of non-witnesses for a general composite odd integer n. We also extend the Miller-Rabin Theorem by determining when the number of non-witnesses $N(n)$ equals $\frac{\varphi(n)}{4}$ and by proving that for all n, if $N(n) > \frac{5}{32} \cdot \varphi(n)$ then n must be of one of the following 3 forms: $n = (2x+1)(4x+1)$, where x is an integer, $n = (2x+1)(6x+1)$, where x is an integer, n is a Carmichael number of the form pqr, where p, q, r are distinct primes congruent to 3 (mod 4). Finally, we find witnesses to certain forms of composite numbers with high rates of nonwitnesses. This work is expected to result in a faster and better primality test for large integers. (Received September 16, 2014)