World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:17, No:12, 2023

An Analysis of Non-Elliptic Curve Based Primality Tests

Authors : William Wong, Zakaria Alomari, Hon Ching Lai, Zhida Li

Abstract : Modern-day information security depends on implementing Diffie-Hellman, which requires the generation of prime numbers. Because the number of primes is infinite, it is impractical to store prime numbers for use, and therefore, primality tests are indispensable in modern-day information security. A primality test is a test to determine whether a number is prime or composite. There are two types of primality tests, which are deterministic tests and probabilistic tests. Deterministic tests are adopting algorithms that provide a definite answer whether a given number is prime or composite. While in probabilistic tests, a probabilistic result would be provided, there is a degree of uncertainty. In this paper, we review three probabilistic tests: the Fermat Primality Test, the Miller-Rabin Test, and the Baillie-PSW Test, as well as one deterministic test, the Agrawal-Kayal-Saxena (AKS) Test. Furthermore, we do an analysis of these tests. All of the reviews discussed are not based on the Elliptic Curve. The analysis demonstrates that, in the majority of real-world scenarios, the Baillie- PSW test's favorability stems from its typical operational complexity of O(log 3n) and its capacity to deliver accurate results for numbers below 2^64.

Keywords : primality tests, Fermat's primality test, Miller-Rabin primality test, Baillie-PSW primality test, AKS primality test
Conference Title : ICDAC 2023 : International Conference on Data Analytics and Cybersecurity
Conference Location : Rome, Italy
Conference Dates : December 11-12, 2023

Open Science Index, Computer and Information Engineering Vol:17, No:12, 2023 publications.waset.org/abstracts/173827.pdf