PROJECT PROPOSAL

Analysis of the Error Probabilities of Miller-Rabin Primality Test

A primality test tries to determine whether or not a given number is prime, without actually decomposing the number into its prime factors. These tests can be divided into two groups: deterministic and probabilistic. In deterministic tests, the output of the algorithm, prime or composite, is certain. Lucas-Lehmer test and elliptic curve primality proving can be given as examples of deterministic tests. The probabilistic tests are generally fast compared to deterministic tests, in these tests, it is possible to identify a composite number as prime with very small error probability, but not vice versa. Fermat test, Solovay-Strassen test and Miller Rabin test can be given as examples of probabilistic tests.

Miller Rabin test, also known as the strong pseudo-prime tests, is based on the following fact.

Fact. Let n be an odd prime, and let $n-1=2^s r$ where r is odd. Let a be any integer such that gcd(a,n)=1. Then either $a^r \equiv 1 \pmod{n}$ or $a^{2^j r} \equiv -1 \pmod{n}$ for some j, 0 ≤ j ≤ s-1.

The pseudo-code of the Miller-Rabin test is given below.

Miller-Rabin (n,t)
INPUT : An odd integer n > 1 and a positive security parameter t
OUTPUT : "Composite" or "Prime"

Write $n-1=2^s r$ such that r is odd
Repeat from 1 to t
    Choose a random integer a which satisfies 1 < a < n - 1
    Compute y = a^r mod n
    If y ≠ 1 and y ≠ n - 1 then DO
        j := 1
        WHILE j < s and y ≠ n - 1 then DO
            y := y^2 mod n
            if y = 1 then return("COMPOSITE")
            j := j + 1
        if y ≠ n - 1 then return("COMPOSITE")

return("PRIME")

Let $p_{k,t}$ be the probability that Miller-Rabin(n,t) state prime for a k-bit composite number after t iteration. A trivial upper bound of this probability is $(1/4)^t$, however this bound can be improved significantly.

In this project, the aim is to make a complete study on the error probality, $p_{k,t}$, of Miller-Rabin test by comparing various bounds available in literature.

References

1. Burthe, R. J., Jr. "Further Investigations with the Strong Probable Prime Test," Mathematics of Computation 65 (1996), pp. 373-381.
2. Damgard, I., Landrock, P., and Pomerance, C. "Average Case Error Estimates for the Strong Probable Prime Test," Mathematics of Computation 61 (1993), pp. 177-194.
3. IEEE Standard Specifications for Public Key Cryptography, IEEE Std 1363, 2000.
4. Menezes, A., van Oorschot, P., and Vanstone, S. Handbook of Applied Cryptography, CRC Press, Boca Raton, Florida, 1996.