MODERNIZATION OF THE SOLOVAY-STRASSEN TEST

Snejana Shegeva

Technical University of Moldova, E-mail: Snej_net@yahoo.com

Abstract: Today's version of the Solovay-Strassen test appears more complicated than the Miller-Rabin test mostly because of the need to compute the Jacobi symbol. This computation is required because the Solovay-Strassen test uses random numbers, which may possibly not be prime, as bases for the testing. However, choosing only prime numbers allows us to avoid the harder implementation of the Jacobi symbol and use instead the Legendre symbol. The calculation of the Legendre symbol can be performed by a simple procedure that computes the residue when a tested number is divided by a base.

Key words: Solovay-Strassen test, Jacobi symbol, Legendre symbol, indicative number.

The question of the relative accuracy of the Solovay-Strassen and Miller-Rabin tests is not only in the sense of the relative correctness of each test on a fixed candidate, but also in the sense than given candidate, the specified containments hold for each randomly chosen base. Thus, from a correctness point of view, the Miller-Rabin test is never worse than the Solovay-Strassen test. There are, however, some composite integers for which Solovay-Strassen and Miller-Rabin test are equally good.

We propose in this article a modernization of the Solovay-Strassen test can give results that are not only never worse but even sometimes better than Miller-Rabin's ones.

Before offering our suggestions let's compare and see some relationships between the two tests and present some differences between them with regard to three considerations: computational cost, implementation and operating speed.

The Solovay-Strassen test appear both computationally and conceptually more complex. While the Miller-Rabin test requires the equivalent of computing $a^{\frac{(n-1)}{2}} \bmod n$, the Solovay-Strassen test also possibly requires a further Jacobi symbol computation, which is a complex procedure.

The mathematical justification of the proposed modernized algorithm is based on the law of quadratic reciprocity:

$$\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)(-1)^{(a-1)(n-1)/4} \quad (1)$$

The classical version of the Solovay-Strassen algorithm can be expressed as follows:

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) (\mathrm{mod}\, n) \quad (2)$$

The Jacobi symbol $\left(\frac{a}{n}\right)$ used in expression (2) is a generalization of the Legendre symbol, where a is required to be a prime number. Hence, taking as bases just prime numbers makes it possible to switch from complex Jacobi number computations to Legendre symbol computations and thus the law of quadratic residue can be applied.

Taking this into account, equation (2) can be transformed to:

$$a^{\frac{n-1}{2}} \equiv \left(\frac{n}{a}\right)^{\frac{(a-1)(n-1)}{4}} (\mathrm{mod}\, n) \quad (3)$$

In equation (3) the reversed symbol $\frac{n}{a}$ corresponds to a simple computational procedure, which replaces the previously used computationally complex procedure of Jacobi symbol computation and erases the advantage of Miller-Rabin test at this point.

Furthermore, the assumed higher speed of the Miller-Rabin in comparison with Solovay-Strassen test is only partially true. This holds for numbers of the form $n = 4k + 1$. However, for numbers of the form $n = 4k - 1$ the Solovay-Strassen test has even an advantage, which was experimentally shown (using about a thousands experiments) with prime numbers forming initial row as bases.

The modernized Solovay-Strassen test gives results with one iteration, when the base $a = 3$, with the exception of strong pseudoprimes.

The conception "critical number of iteration" first appears in the proposed modernized algorithm and it means that for each number group there is a proper strong pseudoprime with own critical (control) value a_{cr} for proving the complexity of the given strong pseudoprime.

For example, strong pseudoprime $1\,373\,653\ (a_{cr} = 5)$ is proper strong pseudoprime for number group with less then 7 digits; $25\,326\,001\ (a_{cr} = 7)$ for number group with less then 8 digits.

This row can be expanded 'till 56th-digits number, because the largest known strong pseudoprime is $6261592193697586271292194012879071219227335876980762017 1$.

Searching for new strong pseudoprimes is undoubtedly a time-taking process, but for practical use we don't have to know their precise values. The only important thing is the value a_{cr} for a given length number.

One can easily notice the dependence a_{cr} from number length, observing the a_{cr}'s changes from previous category to next one. Thus, the empiric dependence between number of iteration k (the number of prime in the prime row) and length of strong pseudoprime n has the following form:

$$k = 0.5 \lg n \quad (4)$$

For example, 10 iterations should be done to test number of the order 10^{20}, who's $a_{cr} = 37$. Boundaries are not crossed, because for the nearest 24^{th}-digits strong pseudoprime 427343918229393756373567 $a_{cr} = 37$, i.e. we still remain within the given range.

For practical needs in cryptography, for example for efficient generation of public key parameters, there is a need to compute primes p and q for an RSA modulus $n = pq$. In this case, the prime must be of sufficient size, and be "random" in the sense that the probability of any particular prime being selected must be sufficiently small to preclude an adversary from gaining the advantage through optimizing a search strategy based on such probability. Both classical and modernized tests have sufficient accuracy in identification of composite number, because the distribution of strong pseudoprime is very scarce (in the range 'till $25 \cdot 10^9$ there are only 5 strong pseudoprimes) and so the chance to "face" the strong pseudoprime has sufficiently small probability for applying in generation of large prime numbers.

REFERENCE

1. Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone, CRC Press, 1996.
2. Olejnik V.L. Methods of deriving of prime numbers - a flowing state - Chişinău.:Akta Akademia All, 1999.
3. Agafonov A.F. The developed probability algorithms of definition of a simplicity of number. - Kishinev: Materials of II International conference on computer science, 2002.
4. Shegeva Sn. "A generation block of prime numbers" – Kishinev: Materials of anniversary scientific conference, 2004.
5. Maslenikov A. Practical cryptography.-M.: SOLON-pres, 2003.