Safe Prime Generation with a Combined Sieve

Michael J. Wiener

Cryptographic Clarity, 20 Hennepin St., Nepean, Ontario, Canada K2J 3Z4
michael.wiener@sympatico.ca

Abstract. A number p is a safe prime if both p and $(p-1)/2$ are prime. This note describes a method of generating safe primes that is considerably faster than repeatedly generating random primes q until $p = 2q+1$ is also prime.

Key words. Safe primes, Prime generation.

1 Introduction

A number p is a safe prime if both p and $(p-1)/2$ are prime. Methods for generating random primes are well-known. One popular method of generating (probable) primes begins by choosing a random odd starting point n and searching for a prime among $n, n+2, n+4, \ldots$ by performing a small prime sieve to eliminate candidates that are divisible by primes smaller than some bound B, and then performing some more expensive test (such as Miller-Rabin [1, Algorithm 4.24]) to determine primality (with high probability) of the remaining candidates.

A simple method of generating safe primes is to repeatedly generate random primes q of the desired size until $p = 2q+1$ is also prime [1, Algorithm 4.86].

Naccache showed how to speed this up by about a factor of two by testing both $2q+1$ and $(q-1)/2$ for primality [2]. However, we show in Section 2 that we can do much better than this by modifying the sieve step in the generation of random primes q.

2 A Faster Method of Generating Safe Primes

An observation that speeds up the safe prime generation method described in the Introduction by a factor of 2 is that both q and $p = 2q+1$ must be congruent to 2 modulo 3 (with the trivial exception of $p = 7$). If either p or q is 1 modulo 3, then the other will be divisible by 3. Thus we can modify the sieve to eliminate not only the candidates for q that are divisible by 3, but also those congruent to 1 modulo 3.

There is no reason to stop there. For any small odd prime r, we can eliminate candidates for q that are congruent to $(r-1)/2$ modulo r because they lead to p being divisible by r.

Let S be the set of odd primes $\leq B$. In the original sieve, $\prod_{r \in S}(r-1)/r$ of the candidates survive the sieve, but this drops to $\prod_{r \in S}(r-2)/r$ in the modified sieve. Thus $\prod_{r \in S}(r-1)/(r-2)$ times fewer candidates for q have to be tested with Miller-Rabin. The sieve change will not change the proportion of candidates for q that turn out to be prime (or at least will change it very little) so that the number of Miller-Rabin tests on candidates for p will be reduced by the same factor. For example, if $B = 2^{16}$, the savings is a factor of approximately 15 (ignoring the cost of the sieve). The actual amount of savings will depend on the relative costs of the sieve and Miller-Rabin steps and the small prime bound used.

It is possible to use Naccache's idea to squeeze out roughly another factor of 2 by modifying the sieve to eliminate all candidates q that lead to $(q-1)/2$, q, or $2q+1$ being divisible by a small prime. Thus q cannot be congruent to 1, 0, or $(r-1)/2$ modulo r for each small prime r. For each remaining q candidate found to be prime, we can test both $(q-1)/2$ and $2q+1$ for primeness to double the chance of success.

3 Conclusion

Using methods described in this note, it is possible to generate safe primes considerably faster than the most obvious approach. In one example where a small prime bound of 2^{16} is used, roughly a factor of 15 is saved in run time.

These methods were implemented by this author more than a decade ago, but it seems doubtful that the ideas were original even then. It is likely that this simple optimization was found by other implementers, but it does not seem to have been published anywhere. This author does not seek to claim credit for originating this idea, but does claim independent discovery.

References

1. A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1997.
2. D. Naccache, Double-Speed Safe Prime Generation, Crypto Eprint Archive entry 2003:175, http://eprint.iacr.org, 2003.