Double-Speed Safe Prime Generation

David Naccache

Gemplus Card International

Applied Research & Security Centre

34 rue Guynemer, Issy-les-Moulineaux, F-92447, France

david.naccache@gemplus.com

Abstract. Safe primes are prime numbers of the form $p = 2q + 1$ where q is prime. This note introduces a simple method for doubling the speed of safe prime generation. The method is particularly suited to settings where a large number of RSA moduli must be generated.

keywords : safe primes, key-generation, prime-generation, RSA.

1 Introduction

Safe primes are prime numbers of the form $p = 2q + 1$ where q is prime. Such primes have various cryptographic advantages, we refer the reader to [1] for further references about safe primes and their applications.

Given a probabilistic prime generation algorithm $\mathcal{A}$ that takes as input a size parameter k and outputs a random prime $2^{k-1} < p < 2^k$ with $p \equiv 3 \bmod 4$, the straightforward way to generate a k-bit safe prime consists of calling $\mathcal{A}$ with different random seeds until both p and $(p-1)/2$ are prime :

$$\texttt{do}(p := \mathcal{A}(k))\ \texttt{while}\ ((p-1)/2\ \texttt{is composite})$$

A well-known result (the prime number theorem [1]), states that the number of primes not exceeding n is approximately $n/\ln n$.

Let $p(k)$ be the probability that k-bit odd integer is prime; applying the prime number theorem, we get :

$$p(k) \simeq \frac{1}{2^{k-2}}\left(\frac{2^k}{k\ln 2} - \frac{2^{k-1}}{(k-1)\ln 2}\right) \simeq \frac{2}{k\ln 2}$$

Assuming that the time complexity of $\mathcal{A}$ (denoted $f(k)$) depends only on k, the overall complexity of the straightforward safe prime generation approach is given by :

$$C(k) = \frac{f(k)}{p(k-1)} \simeq \frac{f(k)k\ln 2}{2}$$

In the following section we will show that this complexity can be divided by a factor of two.

2 The new technique

The idea consists in testing the primality of both $2p+1$ and $(p-1)/2$ for every prime generated by $\mathcal{A}$.

Hence the new algorithm is :

$$\texttt{do(}p := \mathcal{A}(k)\texttt{) while ((}p-1)/2 \texttt{ and } 2p+1 \texttt{ are composite)}$$

The probability $p'(k)$ that either $(p-1)/2$ or $2p+1$ is prime is given by :

$$p'(k) = 1 - \big(1 - p(k-1)\big)\big(1 - p(k+1)\big) \simeq 2p(k)$$

Hence the overall complexity of this new algorithm is given by :

$$C'(k) = \frac{f(k)}{p'(k)} = \frac{f(k)k\ln 2}{4} = \frac{1}{2}C(k)$$

The complexity of safe prime generation is thus divided by two at the cost of generating primes of size k *or* $k+1$ with equal probability. The generation of RSA moduli of a prescribed length $2k$ can thus be efficiently batched (for instance in a smart-card personalization facility) by sorting the primes into two separate files (F_k containing k-bit primes and F_{k+1} containing $(k+1)$-bit ones). Starting the same generation procedure again for k and $k-1$, we obtain two other files (F'_k and F'_{k-1}) containing k-bit and $(k-1)$-bit primes. $2k$-bit RSA moduli are then be formed by picking primes in $\{F'_k, F_k\}$ or in $\{F'_{k-1}, F_{k+1}\}$.

References

1. A. Menezes, P. van Oorschot & S. Vanstone, *Handbook of applied cryptography*, CRC Press, pp. 64 and 164.