HAL
open science

A new method for the generation of strong prime numbers

Yannick Saouter

To cite this version:

Yannick Saouter. A new method for the generation of strong prime numbers. [Research Report] RR-2657, INRIA. 1995. inria-00074032

HAL Id: inria-00074032

https://inria.hal.science/inria-00074032

Submitted on 24 May 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

A new method for the generation of strong prime numbers

Yannick Saouter

N° 2657

Septembre 1995

PROGRAMME 1

Rapport de recherche

ISSN 0249-6399

A new method for the generation of strong prime numbers

Yannick Saouter†

Programme 1 — Architectures parallèles, bases de données, réseaux et systèmes distribués
Projet API

Rapport de recherche n° 2657 — Septembre 1995 — 12 pages

Abstract: Since the discovery of the RSA encryption scheme, primality domain has gained much interest. For the generation of keys for this code, two prime numbers are used. Amongst the different methods to deal with this problem, we are here interested in generation of certified prime numbers and we present a new method less costly in terms of computation in regard of the other methods of generation for a given size of prime numbers.

Key-words: Cryptography; Prime number generation

(Résumé : tsvp)

† email: **saouter@irisa.fr**

Unité de recherche INRIA Rennes
IRISA, Campus universitaire de Beaulieu, 35042 RENNES Cedex (France)
Téléphone : (33) 99 84 71 00 – Télécopie : (33) 99 84 71 71

Une nouvelle méthode de génération de nombre premiers robustes

Résumé : Depuis l'invention du schéma d'encryption RSA, le domaine de la primalité a connu un regain d'intérêt. Pour la génération des clés de ce code, deux nombres premiers sont utilisés. Parmi les différentes methodes pour aborder ce problème nous nous intéressons ici a la génération de nombres premiers certifiés et nous présentons une nouvelle méthode moins coûteuses en temps de calcul par rapport aux autres méthodes de génération pour une taille donné des nombres premiers souhaités.

Mots-clé : Cryptographie; Génération de nombre premiers

1 Introduction

Primality domain has gained much interest with the cryptographic RSA encryption scheme[1]. This method uses a key N which is the product of two prime numbers. The security of the code is insured by the fact that the reverse factorization of N is practically impossible. Some cryptographists generate keys by multiplying two prime numbers certified by one exact primality test [2, 3]. This method has essentially the disavantadge that random prime numbers cannot be certified in a reasonnable time on monolithic machines when they exceed 300 digits. Some other cryptographists use on the contrary pseudo-primality tests : those tests are much less costly in terms of computation. One may cite for example Solovay-Strassen test [4], Miller-Rabin test [5] and Baillie-Wagstaff method [6]. Here the disavantage is clearly the doubt, although extremely reduced, on the effective primality of the numbers selected. Another method in use is the generation of certified prime numbers. These methods enable to build numbers [7, 8] whose primality is established without any doubt. In fact, these methods have generally a cost of computation smaller in regard of the two previous family of methods. Indeed, for example, Maurer's method [8] has a cost slightly greater than a unique Miller-Rabin test which is not safe enough if only applied once. In this article we present a new method which belongs to this last set and which have a reduced complexity and a greater variety in the prime numbers generated, in regard of the other methods of prime generation.

2 Motivations

The problem we have here is to generate two prime numbers p and q such that their product $N = pq$ is hard to factorize back. As a consequence the number N has to resist to all classical factorization techniques. At first this number should be prevented from trial division. This property is ensured by taking large numbers for p and q. Moreover if sufficient prime factors of $p-1$ and $q-1$ or respectively $p+1$ and $q+1$ are known two techniques [9, 10] enables the reverse factorization of N. Practically the programs assume that those numbers have sufficiently small factors and go on adding candidate factors until the list enables the factorization of N. As a consequence in order to resist those methods the two prime numbers p and q have to be such that $p \pm 1$ and $q \pm 1$ have a sufficient number of large factors. Another well known heuristical technique is Pollard's rho method[11]. Without any assumption on the prime factors p and q, a conjecture[12] states that this method find the least factor p of a number N in $(\pi/8)^{1/2}\sqrt{p}$ iterations in average. Then again in order to resist this method, the prime factors of N have to be large.

3 Definitions

Definition 3.1 (Kronecker's symbol) *Let i and j be two integers, the* Kronecker's symbol *denoted δ_i^j is defined to be equal to 1 if $i = j$ and 0 on the case of the contrary.*

Definition 3.2 (Legendre's symbol) *Let a be an integer and p a prime number. Then the* Legendre's symbol, *denoted $(\frac{a}{p})$ or also $L(a,p)$, is defined to be equal to $+1$ if there exists an integer b such that $b^2 = a$ [mod. p] and is equal to -1 is no such integer exists.*

Definition 3.3 (Jacobi's symbol) *Let a and b be two integers relatively prime with each other. The* Jacobi's symbol, *denoted $(\frac{a}{b})$ or also $J(a,b)$, is equal to $\prod_{p|b} L(a,p)^{e_p}$ where $\mid b \mid = \prod_{p|b} p^{e_p}$ is the canonical factorization of $\mid b \mid$ into prime factors p.*

Jacobi's and Legendre's symbol coincide if the denominator is a prime number and thus the fractional notation is not confusing. The Jacobi's symbol verifies the following properties :

Theorem 3.1 *Let a, a', b and b' be four integers then we have :*

$$\begin{array}{lcl}
(\frac{a.a'}{b}) & = & (\frac{a}{b}).(\frac{a'}{b}) \\
(\frac{a}{b.b'}) & = & (\frac{a}{b}).(\frac{a}{b'}) \\
(\frac{a \ mod \ b}{b}) & = & (\frac{a}{b}) \\
(\frac{-1}{b}) & = & (-1)^{(b-1)/2} \\
(\frac{2}{b}) & = & (-1)^{(b^2-1)/8} \\
(\frac{a}{b}) & = & (-1)^{(a-1)(b-1)/4}(\frac{b}{a}) \ a, b \text{ odd and } (a,b) = 1
\end{array}$$

With these properties the computation of $J(a,b)$ does not require the factorizations of a nor b.

Definition 3.4 (Lucas sequence) *Let P and Q be two integers such that $D = P^2 - 4Q \neq 0$. The* principal Lucas sequence *associated to the pair (P,Q) is defined by the following recurrence equations:*

$$\begin{aligned} U_0(P,Q) &= 0 \\ U_1(P,Q) &= 1 \\ U_{n+2}(P,Q) &= P.U_{n+1}(P,Q) - Q.U_n(P,Q) \end{aligned}$$

The companion Lucas sequence *associated to the pair (P,Q) is defined by the following recurrence equations:*

$$\begin{aligned} V_0(P,Q) &= 2 \\ V_1(P,Q) &= P \\ V_{n+2}(P,Q) &= P.V_{n+1}(P,Q) - Q.V_n(P,Q) \end{aligned}$$

The integer D is called discriminant *of the Lucas sequence U_n.*

Theorem 3.2 *Let U_n and V_n be the Lucas sequences associated to the pair (P,Q). Then we have:*

$$\begin{pmatrix} U_n & V_n \\ U_{n-1} & V_{n-1} \end{pmatrix} = M^{n-1} \begin{pmatrix} 1 & P \\ 0 & 2 \end{pmatrix}$$

where $M = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}$.

This theorem enables to compute the terms of a Lucas sequence by the classical binary method.

4 Criteria of primality

The first significant result in the domain of primality belongs to Lucas [13] :

Theorem 4.1 *Let N be an integer. The number N is a prime number if and only if there exists an integer a relatively prime with N such that $a^{N-1} = 1$ [mod. N] and $a^{(N-1)/m} \neq 1$ [mod. N] for any divisor m of $N-1$.*

A refinement of this theorem was done by Brillhart et al.[14] but the main problem with these theorems is the total factorization of $N-1$ is required. This theorem was used by Knuth to prove primality [15] and by Gordon to generate certified prime numbers [7]. A refinement of this theorem [16] uses partial factorization of $N-1$ and was used by Maurer[8] to design a method of generation of prime numbers.

Another family of theorems uses the factorization of $N+1$. The basic theorem is due to Lehmer [17] :

Theorem 4.2 *Let N be an integer. The number N is a prime number if and only if there exists a Lucas's series U_m such that $U_{N+1} = 1$ [mod. N] and $U_{(N+1)/r_i} \neq 1$ [mod. N] for all the prime divisors r_i of $N+1$.*

This theorem also enables to build a prime certificate using Knuth's method — although none implementation seems to have been done. As with the previous theorem, it was proven that only partial factorization of $N+1$ is sufficient [14].

In fact the partial factorizations of $N-1$ et $N+1$ may be used together in order to prove primality. In [14] the following theorem is proven:

Theorem 4.3 *Let N be an odd integer, F_1 the complete factorized part of $N-1$ and F_2 the complete factorized part of $N+1$. We pose $\bar{F}_2 = F_2/2$, $R_1 = (N-1)/F_1$ and $R_2 = (N+1)/F_2$. We suppose moreover $(R_1, F_1) = (R_2, F_2) = 1$. Let us suppose that we have :*

- *(A) for each prime divisor q_i of F_1, there exists an integer a_i such that:*

$$a_i^{N-1} = 1 \text{ [mod. } N] \text{ and } (a_i^{(N-1)/q_i} - 1, N) = 1$$

- *(B) there exists an integer a such that:*

$$a^{N-1} = 1 \text{ [mod. } N] \text{ and } (a^{(N-1)/R_1} - 1, N) = 1$$

- *(C) for each prime divisor r_i of F_2, there exists a Lucas series (u_k^i) whose discriminant D' (the value of the discriminant is common to all the series considered) is such that $(\frac{D'}{N}) = -1$ and:*

$$N \mid u_{N+1}^i \text{ and } (u_{(N+1)/r_i}^i, N) = 1$$

- *(D) there exists a Lucas series (u_k) whose discriminant D' is such that $(\frac{D'}{N}) = -1$ and such that:*

$$N \mid u_{N+1}^i \text{ and } (u_{(N+1)/R_2}^i, N) = 1$$

Moreover we suppose that all the prime factors R_1 and R_2 are respectively greater than B_1 and B_2 respectively. We define r and s by $R_1 = \bar{F}_2 s + r$, and let :

$$G = max(B_1F_1 + 1, B_2F_2 - 1, mF_1\bar{F}_2 + rF_1 + 1) \text{ with } (m \geq 1).$$

Moreover, in the case that $G = mF_1\bar{F}_2 + rF_1 + 1$, we assume $(\lambda F_1\bar{F}_2 + rF_1 + 1) \not| N)$ for all integer λ, $\delta_0^r \leq \lambda < m$, where δ_0^r is the Kronecker symbol. Then if $N < G(B_1B_2F_1\bar{F}_2 + 1)$, N is a prime number.

From the theorems 4.1 and 4.2, it is clear that the converse of the latter theorem is true (although useless).

5 Systems of congruence

This paragraph is devoted to describe the set of integers N such that $N - 1$ and $N + 1$ are constrained to have determined large prime factors. If A (resp. B) is an odd divisor of $N - 1$ (resp. $N + 1$) then we have $N = 1$ $[mod.\ A]$ (resp. $N = -1$ $[mod.\ B]$).

We will use the Bezout's theorem:

Theorem 5.1 *Let A and B be two non-null positive integers relatively prime. Then there exists two integers u and v such that $Au - Bv = 1$.*

These numbers may be computed by the classical Euclid's algorithm[15].

First of all, we can remark that A and B are necessarily relatively prime. Indeed if d is the greatest common divisor of A and B then it necessarily divides $N - 1$ and $N + 1$, and whence the difference, i.e. 2. But d is necessarily odd, since A and B are, and then $d = 1$.

Since N is searched in order to be prime, both $N - 1$ and $N + 1$ are constrained to be divisible by 2. Let 2^k be the greatest power of 2 that divides $N - 1$. If $k \geq 2$, then $N - 1$ is divisible by 4 and $N + 1$ is not. Reciprocally if $N + 1$ is divisible by 2^k with $k \geq 2$, then the greatest power of 2 which divides $N - 1$ is 2.

So we are here concerned with two kinds of systems of congruence :

$$\begin{cases} N = 1 \ [mod.\ 2^k.A] \\ N = -1 \ [mod.\ B] \end{cases} \quad (I)$$
$$\begin{cases} N = 1 \ [mod.\ A] \\ N = -1 \ [mod.\ 2^k.B] \end{cases} \quad (II)$$

Theorem 5.2 *Let u and v be integers such that $Au - Bv = 1$ and let r and s be integers such that $2^k r - Bs = 1$ then N is solution of the system (I) if and only if $N = 1 - ur2^{k+1}A$ $[mod.\ 2^kAB]$.*

Proof Let N be an integer congruent to 1 modulo 2^kA. We pose $N = 1 + k_1 2^k A + k_2 2^k AB$ with $0 \leq k_1 \leq B - 1$. We determine u, v, r and s as stated in the hypothesis of the theorem. We have then $(N - 1)u = k_1 2^k Au + k_2 2^k ABu$. We have $Au = 1 + Bv$ and so $(N - 1)u = k_1 2^k(1 + Bv) + k_2 2^k ABu$. We have then $(N - 1)u = k_1 2^k$ $[mod.\ B]$. By multiplying by r we obtain $(N - 1)ur = k_1 2^k r$ $[mod.\ B]$, so $(N - 1)ur = k_1(1 + Bs)$ $[mod.\ B]$ so $k_1 = (N - 1)ur$ $[mod.\ B]$. N is solution of system (I) if and only if $N = -1$ $[mod.\ B]$. As a consequence N is solution if and only if $k_1 = -2ur$ $[mod.\ B]$. Finally we have $N = 1 + k_1 2^k A$ $[mod.\ 2^kAB]$ so $N = 1 - ur2^{k+1}A$ $[mod.\ 2^kAB]$. □

Theorem 5.3 *Let u and v be integers such that $Au - Bv = 1$ and let r and s be integers such that $2^k r - As = 1$ then N is solution of the system (II) if and only if $N = -1 + rv2^{k+1}B$ $[mod.\ 2^kAB]$.*

Proof Same as above. □

Given those two theorems, it is possible to search for integers N such that $N+1$ and $N-1$ have specified divisors. With the use of theorem 4.3, whenever the product of the factorized parts of $N-1$ and $N+1$ exceed the square root of N then the primality of N can be established.

In both cases the congruence which is finally obtained proves that N necessarily belongs to an arithmetic progression whose first term and ratio are relatively prime. Indeed for instance in theorem 5.2, if we suppose that N and $2^k AB$ are not relatively prime then they have a common divisor $d = 2^l.a.b$ where $0 \leq l \leq k$ and a (resp. b) is a divisor of A (resp. B). If we put $N = 2^l.a.b.N_0$, we have then $N = 2^l.a.b.N_0$ $[mod.\ 2^k.A]$ and $N = 2^l.a.b.N_0$ $[mod.\ B]$. But we have also by hypothesis $N = 1$ $[mod.\ 2^k.A]$ and $N = -1$ $[mod.\ B]$. So we have $2^l.a.b.N_0 = 1$ $[mod.\ 2^k.A]$ and $2^l.a.b.N_0 = -1$ $[mod.\ B]$. Then by Bezout's theorem, $2^l.a.b.N_0$ is relatively prime with both $2^k.A$ and B. So necessarily $l = 0$ and $a = b = 1$, and thus $d = 1$, i.e. N and $2^k AB$ are relatively prime. As a consequence $2^k.A.B$ and the first term of the progression are also relatively prime.

At this point Dirichlet's result applies [18] and necessarily such an arithmetical progression contains a prime number and whence an infinite number of prime numbers. Moreover it has been proven by Linnik[19] and Chen[20] that the least prime number in an arithmetical progression $a + k.d \mid \ k \leq 0$ where a and d are relatively prime is overestimated by d^{17}.

In practice the first prime number in the sequence is much smaller. Indeed let N belongs to an arithmetical progression as above. Then if we suppose that the terms of the progression can independently be prime, by LaVallé theorem[21, p. 164], the probability that N is prime is roughly equal to $\frac{1}{log\ N}$, i.e. roughly $\frac{1}{log\ d}$ if k is small in regard of d. So probabilistically the least prime number is obtained for a rank k of the same order of size that $log\ d$. This idea is confirmed by a result of Wagstaff[22].

6 Numerical example

In this section, we illustrate this new method by a numerical example. In order to choose our Lucas sequences we follow the Baillie's rule [6]: D is the first integer in the sequence 5, 9, 13, 17, ... such that $J(D,p) = -1$ and take P as the least odd number greater than $\sqrt{D}$. If this value fails increment by 2. After several unsuccessful attempt, discard p.

As for example, we will search here for a prime number p which will be constrained to the follwing congruences:

$$\begin{array}{lcll}
p & = & 1 & [mod.\ 16] \\
p & = & 1 & [mod.\ 47162591668545133312394804947079119 1639] \\
p & = & 1 & [mod.\ 51703443661991040337511173547191855046621] \\
p & = & -1 & [mod.\ 49624820179289647669758318327131425171 97] \\
p & = & -1 & [mod.\ 99603302763478708108175450119307141223 77]
\end{array}$$

Our system is here of type (I) with $k = 4$,

$$\begin{array}{lcl}
A & = & 2438468401288111316818235741065986243320232256699 8\backslash\backslash \\
 & & 18360327226503198265649040181 9
\end{array}$$

and

$$\begin{array}{lcl}
B & = & 4942795988900974522909109868016031430097410443610 8\backslash\backslash \\
 & & 4412151895409708537304850172 69.
\end{array}$$

The numbers A and B are respectively the product of all the modulo giving a remainder equal to 1 and -1. With the notations of theorem 5.2 we have then

$$\begin{array}{lcl}
u & = & 7004524591591647639514754014180003773497723413673 5\backslash\backslash \\
 & & 3640734027140603507420301987 57, \\
v & = & 3455597180420860381918801785042163131245697106725 0\backslash\backslash \\
 & & 9054982300319371535345623680 78, \\
r & = & 9267742479189327230454581002530058931432644581770 3\backslash\backslash \\
 & & 3272784803893203507446594073 8
\end{array}$$

and $s = 3$. So according to theorem 5.2 this global system is equivalent to the single congruence:

$$\begin{array}{lcl}
p & = & 1827907092277921822237249309047728176925564681521 9\backslash\backslash \\
 & & 5907039550962768161940162925060078077688595253334 2\backslash\backslash \\
 & & 1886786673050289109492184057007471488801869610208 6\backslash\backslash \\
 & & 98623543633\ [mod.\ 16 * A * B]
\end{array}$$

This congruence gives us an arithmetic progression of numbers, which is exactly the set of the solutions of the initial system. In this example the first value suspected to be prime is the 644-th term:

$$\begin{aligned} N \;=\; & 1243753759959306668759016148640093177198836280897 6\backslash\backslash \\ & 4787702050111296172582086993494058896171535386 2000\backslash\backslash \\ & 5706714935272357522307671194369461147728490950 2645\backslash\backslash \\ & 62567806396177. \end{aligned}$$

The selection of this value may be done by the verification of the congruence $a^{N-1} = 1\ [mod.\ N]$ for a given basis. This certificate called Fermat's congruence also belongs to the hypothesis of the theorem. Here a value of $a = 13$ is convenient and passes the test.

```
> N:=1243753759959306668759016148640093177198836280897\
> 7719883628089764787702050111296172582 0\
> 8699349405889617153538620005706714935 2\
> 7235752230767119436946114772849095026 45625678 06396177;

N :=

1243753759959306668759016148640093177198836280897647877020501112961725820869 93\
4940588961715353862000570671493527235752230767119436946114772849095026456256 78\
06396177

> MODEXP(13,N-1,N);

                                    1

>
```

Moreover this number also passes the more complete Miller-Rabin test for the same basis. With the hypothesis of the theorem we have $F_1 = 16 * A$, $F_2 = 2 * B$. The value of R_1 and R_2 are here:

$$\begin{aligned} R_1 \;=\; & 3187845696765792233136800159352069775869904697007 7\backslash\backslash \\ & 3662184399772795644690363929908 19, \\ R_2 \;=\; & 1258147982186752164571699585785651283864447297972 1\backslash\backslash \\ & 0374670989929798125336612401419781. \end{aligned}$$

It is easy to verify that we have $(F_1, R_1) = (F_2, R_2) = 1$. Since we do not intend to factorize much R_1 and R_2, we only take $B_1 = B_2 = 2$. At this point it is possible to verify that the first condition of the theorem is met by taking in any case $a_i = 13$ for the prime factors of F_1 except 2. The reason for this latter fact is that $J(13, N) = 1$ (see the Solovay-Strassen test for detailed explanation). But we have $J(7, N) = -1$ and this basis meet the condition for the prime factor 2.

```
> MODEXP(13,(N-1)/4716259166854513331239480494707911916 39,N);

4882254728053983509678161721510634198539835271329523762812873146430950687705 52\
7845720079463032059145564039589791799622741362649887807918460580110751978694 51\
649714

> igcd("-1,N);

                                    1

> MODEXP(13,(N-1)/2,N);

                                    1

> jacobi(13,N);

                                    1

> jacobi(7,N);

                                   -1

> MODEXP(7,(N-1)/2,N);
```

```
1243753759959306668759016148640093177198836280897647877020501112961725820 86993\
4940588961715353862000570671493527235752230767119436946114772849095026456256 78\
06396176

> igcd("-1,N);

                                        1

>
```

The basis 13 also meet the second condition of the theorem.

At this point if we follow Baillie's rule, we choose $D = 5$, $P = 3$ and $Q = 1$. The prime factors of F_2 are 2, 4962482017928964766975831832713142517197 and 9960330276347870810817545011930714122377. This Lucas sequence holds the condition for the prime factors of F_2 except for 2. The next couple of parameters to be considered is then $P = 5$ and $Q = 5$. This sequence verifes the condition for the prime factor 2.

```
> N:=1243753759959306668759016148640093177198836280897647877020501112961725820 86993\
> 7719883628089764787702050111296172582086993\
> 8699349405889617153538620005706714935 2\
> 7235752230767119436946114772849095026456256 7806396177;

N :=

1243753759959306668759016148640093177198836280897647877020501112961725820 86993\
4940588961715353862000570671493527235752230767119436946114772849095026456256 78\
06396177

> jacobi(N,5);

                                       -1

> lucas(N+1,3,1,N);

                                    [0, 2]

> lucas((N+1)/4962482017928964766975831832713142517197,3,1,N);

[

5613177585414083560514320120447493047663032994042359480402703409367469742477 30\
0820313268218167162910214893938197832188306996350981125878471639665486287826 91\
2933759

    ,

4393669485936067036787842625682559943730107467759976372467087985162620612986 17\
8663606953268596595387445379096849332642888660108389779901111590981622641562 52\
8921688

]

> igcd("[1],N);

                                        1
> lucas((N+1)/2,3,1,N);

[0,

1243753759959306668759016148640093177198836280897647877020501112961725820 86993\
4940588961715353862000570671493527235752230767119436946114772849095026456256 78\
06396175

]

> lucas((N+1)/2,5,5,N);
                                    [2, 0]

> igcd("[1],N);

                                        1
```

```
> lucas((N+1),5,5,N);

                                  [0, 10]

>
```

Again the first Lucas sequence meet the fourth condition of the theorem. Now if we take $m = 1$, we obtain:

$$\begin{aligned} G \quad = \quad & 37563633855497055907726202707418981288229415700563\backslash\backslash \\ & 16085845984167020197354219787386476710020219473508\backslash\backslash \\ & 69253396988256109001725862469336417935218837106036\backslash\backslash \\ & 58047740609 \end{aligned}$$

With this value we verify that the inequation $N < G(4F_1\bar{F}_2 + 1)$ holds. Moreover $r \neq 0$ and since $m = 1$, there is no possible value for λ and thus we can certify that N is effectively a prime number. This example has been treated in Maple[23] sessions. With such a system it is then possible to build certified prime numbers with hundreds of digits in a reasonnable time. The verification indeed takes about an hour. The generation of the prime number (i.e. the search for the least value giving a prime number) is much more costly and takes several hours. However with the use of multiprecision packages it is possible to generate much larger prime numbers. For instance with using a restriction of theorem 5.2, it was possible to certify the number $M_{2281} * (M_{2281} - 1713) + 1$, where $M_{2281} = 2^{2281} - 1$ is known to be a Mersenne prime, as to be also a prime number in 13 hours of computations on a SparcStation 10. This number has 1374 decimal digits.

7 Conclusion

In this article, we have presented a method for the generation of prime numbers. This method allows to fix certain divisors of $N - 1$ and $N + 1$, and thus to insure the difficulty of factorization of the keys of the RSA scheme. A prime number p generated by the method of [8] can also be designed to be "$p + 1$-resistant", by solving a congruence system. However, our method also uses the factors of $p + 1$ in order to prove the primality of p. As a consequence it is possible to certify larger prime numbers with less computation. Indeed the theorem used by Maurer is a restriction of theorem 5.2 which does not use Lucas sequences, and it is then possible to certify only numbers $N < F_1^2$. The method exposed here can certify here at least numbers $N < (F_1\bar{F}_2)^2$ and then is more efficient.

References

[1] R.L. Rivest, A. Shamir, and L.M. Adleman. – A method for obtaining digital signatures and public-key cryptosystems. – *Comm. ACM*, 1978.

[2] L.M. Adleman, C. Pomerance, and R.S. Rumely. – On distinguishing prime numbers from composite numbers. – *Annals of Math.*, 1983.

[3] A.O.L. Atkin and F. Morain. – Elliptic curves and primality proving. – *Math. Comp.*, 61(203), 1993.

[4] R. Solovay and V. Strassen. – A fast Monte-Carlo test for primality. – *SIAM J. Comput.*, 1977.

[5] G.L. Miller. – Riemann's hypothesis and tests for primality. – *J. Comp. Syst. Sci.*, 13, 1976.

[6] R. Baillie and S.S. Wagstaff. – Lucas pseudoprimes. – *Math. Comp.*, 35, 1980.

[7] J. Gordon. – Strong primes are easy to find. – In *LNCS 209. Eurocrypt 84*, pages 216–223, 1984.

[8] U.M. Maurer. – Fast generation of prime numbers and secure public-key cryptographic parameters. – To appear in *Journal of Cryptology*, 1995.

[9] J.M. Pollard. – Theorems on factorization and primality testing. – *Proc. Cambridge Philos. Soc.*, 76:521–528, 1974.

[10] H.C. Williams. – A $p + 1$ method of factoring. – *Math. Comp.*, 39(159):225–234, 1982.

[11] J.M. Pollard. – A Monte-Carlo method for factorization. – *BIT*, 15:331–334, 1975.

[12] R.P. Brent and J.M. Pollard. – Factorization of the eighth Fermat number. – *Math. Comp.*, 36(154):627–630, 1981.

[13] E. Lucas. – *Théorie des Nombres.* – Gauthier-Villars, 1891.

[14] J. Brillhart, D.H. Lehmer, and J.L. Selfridge. – New primality criteria and factorizations of $2^m \pm 1$. – *Math. Comp.*, 29, 1975.

[15] D.E. Knuth. – *Art of Computer Programming : Sorting and Searching.* – Addison-Wesley, 1973.

[16] H.C. Pocklington. – The determination of the prime and composite nature of large numbers by Fermat's theorem. – *Proc. Cambridge Philos. Soc.*, 1914.

[17] D.H. Lehmer. – An extended theory of Lucas' functions. – *Annals of Math.*, 31:419–448, 1930.

[18] G.L. Dirichlet. – Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Gleid und Differenz ganze Zahlen ohne gemeinschatlichen Factor sind, unendlich viele Primzahlen enthält. – *Abh. d. Königl. Akad. d. Wiss.*, 1837.

[19] Y.V. Linnik. – On the least prime in an arithmetic progression i. the basic theorem. – *Mat. Sbornik*, 15(57), 1944.

[20] J.R. Chen. – On the least prime in an arithmetic progression and theorems concerning the zeros of Dirichlet's l-functions. – *Sci. Sinica*, 22, 1979.

[21] P. Ribenboim. – *The Book of Prime Number Records.* – Springer-Verlag, 1988.

[22] S.S. Wagstaff. – Greatest of the least primes in arithmetic progressions having a given modulus. – *Math. Comp.*, 33, 1979.

[23] B.W. Char, K.O. Geddes, and G.H. Gonnet. – *First leaves: a tutorial introduction to MAPLE V.* – Springer-Verlag, 1992.

A Maple script

This section exhibits the Maple listings used to deal with our examples:

```
MODEXP:= proc(a,b,n)
# computes a^b mod n for large numbers
local ret:
if modp(b,2) = 0 then
                    if b=0 then
                             ret:=1:
                           else
                             ret:= modp(MODEXP(a,b/2,n)^2,n):
                    fi:
                  else
                    ret:= modp(a*MODEXP(a,(b-1)/2,n)^2,n):
fi:
RETURN(ret):
end:

bezout:=proc(U)
# takes a vector [A,B] of positive integers and returns
# a vector of integers [u,v] such that Au-Bv=1
local q,r,u,v,V:
if (U[2]=1) then:
        u:=1: v:=U[1]-1:
else if (U[1]=1) then:
        u:=U[2]+1: v:=1:
```

```
else if (U[1]>=U[2]) then:
        r:=U[1] mod U[2]:
        q:=(U[1]-r)/U[2]:
        V:=bezout([r,U[2]]):
        u:=V[1]: v:=V[2]+q*V[1]:
else:
        V:=bezout([U[2],U[1]]);
        r:=V[2] mod U[2]:
        q:=(V[2]-r)/U[2]:
        q:=q+1:
        u:=U[2]*q-V[2]: v:=q*U[1]-V[1]:
fi: fi: fi:
RETURN([u,v]);
end:

jacobi := proc(a,b)
# Computes the jacobi symbol
# (Note: there exists also an implementation
# in a standard package of Maple)
local temp,ret:
if (b=1) then:
ret:=1;
else if (modp(b,2)=0) then:
ret:=jacobi(a,b/2):
else if (igcd(a,b)>1) then:
ret:=0:
else if (a=2) then:
temp:=modp((b^2-1)/8,2):
ret:=1-2*temp:
else if (modp(a,2)=0) then:
ret:=jacobi(a/2,b)*jacobi(2,b):
else if (a>b) then:
ret:= jacobi(a mod b,b):
else:
temp:=modp((a-1)*(b-1)/4,2):
ret:=(1-2*temp)*jacobi(b,a):
fi: fi: fi: fi: fi: fi:
RETURN(ret):
end:



puissmat:=proc(n,M,Modu)
# Computes matrix M^n with modulo Modu
local temp,temp2,ret,a11,a12,a21,a22,ta11,ta12,ta21,ta22:
if (n=0) then:
ret:=[1,0,0,1];
else if (modp(n,2)=0) then:
temp:=puissmat(n/2,M,Modu);
a11:=(temp[1]*temp[1]+temp[2]*temp[3]) mod Modu:
a12:=(temp[1]*temp[2]+temp[2]*temp[4]) mod Modu:
a21:=(temp[3]*temp[1]+temp[4]*temp[3]) mod Modu:
a22:=(temp[3]*temp[2]+temp[4]*temp[4]) mod Modu:
ret:=[a11,a12,a21,a22]:
else:
temp:=puissmat((n-1)/2,M,Modu);
a11:=(temp[1]*temp[1]+temp[2]*temp[3]):
```

```
a12:=(temp[1]*temp[2]+temp[2]*temp[4]):
a21:=(temp[3]*temp[1]+temp[4]*temp[3]):
a22:=(temp[3]*temp[2]+temp[4]*temp[4]):
ta11:=(a11*M[1]+a12*M[3]) mod Modu:
ta12:=(a11*M[2]+a12*M[4]) mod Modu:
ta21:=(a21*M[1]+a22*M[3]) mod Modu:
ta22:=(a21*M[2]+a22*M[4]) mod Modu:
ret:=[ta11,ta12,ta21,ta22]:
fi:
fi:
RETURN(ret);
end:

lucas:=proc(n,P,Q,Modu)
# Computes the n-th term of both Lucas sequences for parameters
# P and Q and with modulo Modu
local temp,temp2,M,M1,ret,u,v:
if (n=0) then:
ret:=[0,2]:
else:
M:=[P,-Q,1,0];
temp:=puissmat(n-1,M,Modu);
u:= temp[1] mod Modu:
v:= (P*temp[1]+2*temp[2]) mod Modu:
ret:=[u,v]:
fi:
RETURN(ret);
end;
```

Unité de recherche INRIA Lorraine, Technopôle de Nancy-Brabois, Campus scientifique,
615 rue du Jardin Botanique, BP 101, 54600 VILLERS LÈS NANCY
Unité de recherche INRIA Rennes, Irisa, Campus universitaire de Beaulieu, 35042 RENNES Cedex
Unité de recherche INRIA Rhône-Alpes, 46 avenue Félix Viallet, 38031 GRENOBLE Cedex 1
Unité de recherche INRIA Rocquencourt, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex
Unité de recherche INRIA Sophia-Antipolis, 2004 route des Lucioles, BP 93, 06902 SOPHIA-ANTIPOLIS Cedex

Éditeur
INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex (France)
ISSN 0249-6399