MATHEMATICAL COMMUNICATIONS
Math. Commun., Vol. **14**, No. 1, pp. 103-118 (2009)

A cryptanalytic attack on the LUC cryptosystem using continued fractions

Bernadin Ibrahimpašić[1,*]

[1] *Pedagogical Faculty, University of Bihać, Džanića mahala 36, 77 000 Bihać, Bosnia and Herzegovina*

Received November 29, 2008; accepted February 20, 2009

Abstract. The LUC cryptosystem is a modification of the RSA cryptosystem based on Lucas sequences. In this paper we extend the Verheul - van Tilborg and Dujella variants of the Wiener attack on RSA to the LUC cryptosystem. We describe an algorithm for finding a secret key d of the form $d = rq_{m+1} \pm sq_m$, for some $m \geq -1$ and nonnegative integers r and s, using continued fractions. We derive bounds for r and s using results on Diophantine approximations.

AMS subject classifications: 94A60, 11A55, 11B39

Key words: cryptanalysis, LUC cryptosystem, diophantine approximations

1. Introduction

In 1978, Rivest, Shamir and Adleman [13] introduced the first practical public–key cryptosystem. This cryptosystem is called RSA. The modulus n of the RSA cryptosystem is the product of two different large primes p and q. The public exponent e and the secret exponent d are related by $ed \equiv 1 \pmod{(p-1)(q-1)}$.

In 1993, Smith and Lennon [14] described a new public–key cryptosystem based on Lucas sequences. The public key is (n, e). The modulus n is the product of two different large primes p and q, and the public encryption key e is relatively prime to the product $(p-1)(q-1)(p+1)(q+1)$.

The public encryption key e and the secret decryption key d are related by

$$ed \equiv 1 \pmod{S(n)}, \tag{1}$$

where there are four possible values for the function $S(n)$:

$$\operatorname{lcm}(p-1, q-1), \quad \operatorname{lcm}(p-1, q+1), \quad \operatorname{lcm}(p+1, q-1), \quad \operatorname{lcm}(p+1, q+1).$$

In 1990, Wiener [16] described a technique to use continued fractions in a cryptanalytic attack on an RSA cryptosystem with a small secret exponent, which is called the Wiener attack. Wiener showed that if $d < n^{0.25}$, then this technique determines d, p and q, since the secret number d is the denominator of some convergent p_m/q_m of the continued fraction expansion of e/n. His result is based on the classical Legendre's theorem on Diophantine approximations of the form $\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$.

[*] Corresponding author. *Email address:* bernadin@bih.net.ba (B. Ibrahimpašić)

In 1999, Boneh and Durfee [3] described an attack on RSA with a small secret exponent d which works if $d < n^{0.292}$. This attack is based on Coppersmith's method [4] for finding small roots to polynomial equations, which is based on the LLL–lattice reduction algorithm. In 2001, Blömer and May [2] proposed a variant of the Boneh and Durfee attack.

In 1997, Verheul and van Tilborg [15] extended the boundary of the Wiener attack on RSA. They propose a technique to raise the security Wiener's boundary of $n^{0.25}$ with exhaustive-searching for $2t+8$ bits, where $t = \log_2 d - \log_2 n^{0.25}$. The candidates for the secret key d are of the form $d = rq_{m+1}+sq_m$, for some nonnegative integers r and s.

In 2004, Dujella [5] described a new variant of the Wiener attack on RSA. His attack is a modification of the Verheul and van Tilborg variant, and it is based on the Worley result on Diophantine approximations [17] of the form $|\alpha - a/b| < c/b^2$, where c is a positive real number. The candidates for the secret exponent d are of the form $d = rq_{m+1} \pm sq_m$, for some nonnegative integers r and s.

In 1995, Pinch [12] extended the Wiener attack to LUC and KMOV cryptosystems, and showed that both cryptosystems with 1024-bit modulus n are insecure for a 256-bit private key d. Note that KMOV is also similar to RSA. This cryptosystem, proposed by Koyama, Maurer, Okamoto and Vanstone [10], uses elliptic curves over the ring $\mathbb{Z}_n$, and its security is based on the difficulty of factoring large integers. KMOV cryptosystem with a 1024-bit modulus n is factoring-secure. Ibrahimpašić [7] showed that in this case, KMOV cryptosystem is insecure for a 270-bit private key d.

In this paper, we generalize the above mentioned attacks which use continued fractions. We extend the Dujella variant of the Wiener attack to the LUC cryptosystem and describe an algorithm for finding a secret key d, where $d = rq_{m+1} \pm sq_m$, for some nonnegative integers r and s. We will show that the LUC cryptosystem with a 1024-bit modulus n is insecure for a 270-bit private key d. We derive bounds for r and s using results on Diophantine approximations [5, 17].

2. Lucas sequences

Let a and b are nonzero integers and α and β the roots of the equation

$$x^2 - ax + b = 0.$$

We have

$$\alpha = \frac{a+\sqrt{\Delta}}{2} \qquad \text{and} \qquad \beta = \frac{a-\sqrt{\Delta}}{2},$$

where $\Delta = a^2 - 4b$.

Lucas sequences (U_n) and (V_n) $(n \geq 0)$ are given by

$$U_n\left(a,b\right) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \ \text{ and } \ V_n = \alpha^n + \beta^n.$$

In particular,

$$U_0 = 0, \quad U_1 = 1, \quad V_0 = 2, \quad V_1 = a,$$

and for $n \geq 2$ we have

$$\begin{aligned} U_n &= aU_{n-1} - bU_{n-2}, \\ V_n &= aV_{n-1} - bV_{n-2} \ . \end{aligned}$$

Note that if $a = 1$ and $b = -1$, then $U_n\left(1,-1\right)$ are the Fibonacci numbers $(0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots)$, and $V_n\left(1,-1\right)$ are the Lucas numbers $(2, 1, 3, 4, 7, 11, 18, 29, 47, \ldots)$.

We have the following relationships [14] between the Lucas sequences V_n, which are easy to prove using the definitions of U_n, V_n, Δ, a and b in terms of α and β:

$$\begin{aligned} V_{2n} &= V_n^2 - 2b^n, & (2) \\ V_{2n-1} &= V_nV_{n-1} - ab^{n-1}, & (3) \\ V_{2n+1} &= aV_n^2 - bV_nV_{n-1} - ab^n, & (4) \\ V_n^2 &= \Delta U_n^2 + 4b^n, & (5) \\ 2V_{n+m} &= V_nV_m + \Delta U_nU_m, & (6) \\ 2b^mV_{n-m} &= V_nV_m - \Delta U_nU_m. & (7) \end{aligned}$$

In further work we need the following relationship [1, 14]

$$V_n\left(V_k\left(a,b\right), b^k\right) = V_{nk}\left(a,b\right),$$

which for $b = 1$ gives

$$V_n\left(V_k\left(a,1\right),1\right) = V_{nk}\left(a,1\right).$$

3. LUC cryptosystem

The LUC cryptosystem is based on Lucas sequences, and it is developed in analogy with the RSA cryptosystem. Suppose n and e are two chosen numbers, where n is the product of two large different primes p and q. The number e must be chosen so it is relatively prime to $\left(p-1\right)\left(q-1\right)\left(p+1\right)\left(q+1\right)$. Let M be a message which is less than n and relatively prime to n. We obtain the ciphertext C by

$$C = V_e\left(M, 1\right) \mod n.$$

The public number e and the secret number d are related by (1) where

$$S\left(n\right) = \operatorname{lcm}\left(p - \left(\frac{C^2-4}{p}\right), q - \left(\frac{C^2-4}{q}\right)\right).$$

The Legendre symbols are either $+1$ or -1 which imply that there are four possible values for $S\left(n\right) = \operatorname{lcm}\left(p \pm 1, q \pm 1\right)$.

Since the choice of public number e ensures that it is relatively prime to $S\left(n\right)$, the secret number d can be found easily by the extended Euclidean algorithm. The decription process is then the same as encryption, with e replaced by d. We have

$$M = V_d\left(C, 1\right) \mod n.$$

By the definition of the Legendre symbol, we have $\left(\frac{\Delta}{p}\right) = \left(\frac{\Delta U_e^2(M,1)}{p}\right)$. Therefore, by (5) we obtain

$$\left(\frac{M^2-4}{p}\right) = \left(\frac{\Delta}{p}\right) = \left(\frac{\Delta U_e^2\left(M,1\right)}{p}\right) = \left(\frac{V_e^2\left(M,1\right)-4}{p}\right) = \left(\frac{C^2-4}{p}\right),$$

which implies [14, 11]

$$U_{kS(n)}\left(C,1\right) \equiv U_{kS(n)}\left(M,1\right) \equiv 0 \pmod{n},$$

$$V_{kS(n)}\left(C,1\right) \equiv V_{kS(n)}\left(M,1\right) \equiv 2 \pmod{n}.$$

Now, we can easily check that the inverse of the encryption function $V_e\left(M,1\right)$ is the decryption function $V_d\left(C,1\right)$ (see [14] for the details).

Computation of V_e and V_d might look extremely long, for large values of e and d. But, in [14] it is shown how this problem can be solved by a modification of the successive doubling technique (see [6, Algorithm 5] or [9, Chapter 4.6.3]).

4. Cryptanalysis of the LUC cryptosystem with a short secret exponent

The security of the LUC cryptosystem is based on the difficulty of finding the secret key d. It was believed that finding a secret key d from public keys e and n is computationally equivalent to factoring a composite number n.

In this paper we are only interested in attacks using continued fractions. Let $\alpha = [a_0; a_1, a_2, \ldots]$ be the continued fractions expansion of a real number α. The convergents $\frac{p_m}{q_m}$ of the continued fraction expansion of α, satisfy $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0 a_1 + 1$, $q_1 = a_1$ and $p_i = a_i p_{i-1} + p_{i-2}$, $q_i = a_i q_{i-1} + q_{i-2}$, for $i > 1$.

In 1990, Wiener [16] proposed a polynomial time algorithm for breaking a typical RSA, where p and q are of the same size and $e < n$. He showed that if $p < q < 2p$, $e < n$ and $d < \frac{1}{3}n^{0.25}$, then d is the denominator of some convergent of the continued fraction expansion of e/n, and therefore d can be computed from the public keys n and e. In 1997, Verheul and van Tilborg [15] proposed an extension of the Wiener attack, which can work well over Wiener's boundary. The candidates for the secret exponent d are of the form $d = rq_{m+1} + sq_m$, for some nonnegative integers r and s. In 2004, Dujella [5] described a modification of the Verheul and van Tilborg variant of the Wiener attack. This attack is very similar to the Verheul and van Tilborg attack, but instead of an exhaustive search after for finding the appropriate convergent, this variant also uses estimates which follow from Diophantine approximations [5, Theorem 1].

Theorem 1 (Dujella, Worley). *Let α be a real number and let a, b be coprime nonzero integers, satisfying the inequality*

$$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2},$$

where c is a positive real number. Then $(a,b) = (rp_{m+1} \pm sp_m, rq_{m+1} \pm q_m)$, for $m \geq -1$ and for some nonnegative integers r, s such that $rs < 2c$.

In 1995, Pinch [12] extended the Wiener attack to the LUC cryptosystem, and here we extend the Dujella variant of the Wiener attack to the LUC cryptosystem.

We assume that $p < q < 2p$ and let $d = D \cdot \sqrt[4]{n}$. The following lemma can be easily proved.

Lemma 1. *Let p, q be two distinct positive odd integers, such that $p < q < 2p$, and $n = pq$. Then*

(i) $2\sqrt{n} < p + q < 2.1214\sqrt{n}$,

(ii) $1.9999 < q - p < 0.7072\sqrt{n}$.

4.1. Case $S(n) = \operatorname{lcm}(p-1, q-1)$

From $ed \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}$ there exists an integer K such that

$$ed = K \cdot \operatorname{lcm}(p-1, q-1) + 1.$$

If we let $G = \gcd(p-1, q-1)$ and use the fact

$$\operatorname{lcm}(p-1, q-1) = \frac{(p-1)(q-1)}{G},$$

we get

$$ed = \frac{K}{G} \cdot (p-1)(q-1) + 1.$$

Let us define

$$k = \frac{K}{\gcd(K,G)} \qquad \text{and} \qquad g = \frac{G}{\gcd(K,G)}.$$

Then $\frac{K}{G} = \frac{k}{g}$, $g < k$ and $\gcd(k, g) = 1$. Also $e < \frac{n}{G}$ and thus $\frac{e}{n} < \frac{1}{G}$. Now we have

$$ed = \frac{k}{g} \cdot (p-1)(q-1) + 1 \quad \Longrightarrow \quad edg = k(p-1)(q-1) + g, \tag{8}$$

and we obtain

$$\frac{k}{dg} - \frac{e}{n} = \frac{kn - edg}{ndg} = \frac{k(p+q) - k - g}{ndg} > \frac{k(p+q) - k - k}{ndg} > \frac{2k(\sqrt{n} - 1)}{ndg}.$$

Since $\frac{k}{dg} > \frac{e}{n} \cdot \frac{n}{n - 2\sqrt{n} + 1}$, we obtain

$$\begin{aligned} \frac{k}{dg} - \frac{e}{n} &> \frac{e}{n} \cdot \frac{n}{n - 2\sqrt{n} + 1} - \frac{e}{n} = \frac{e}{n} \cdot \frac{2\sqrt{n} - 1}{\left(\sqrt{n} - 1\right)^2} \\ &> \frac{e}{n} \cdot \frac{2\left(\sqrt{n} - 1\right)}{\left(\sqrt{n} - 1\right)^2} = \frac{e}{n} \cdot \frac{2}{\sqrt{n} - 1} > \frac{2e}{n\sqrt{n}}. \end{aligned}$$

In the opposite direction we have

$$\frac{k}{dg} - \frac{e}{n} = \frac{kn - edg}{ndg} = \frac{k(p+q) - k - g}{ndg} < \frac{k(p+q)}{ndg} < \frac{2.1214k\sqrt{n}}{ndg} < \frac{2.1214k}{dg\sqrt{n}}.$$

We may assume that $n > 10^8$. Then we have

$$\begin{aligned}\frac{k}{dg}-\frac{e}{n} &< \frac{2.1214k}{dg\sqrt{10^8}}=\frac{0.00021214k}{dg}\implies \frac{e}{n}>\frac{k-0.00021214k}{dg}\\ &\implies \frac{k}{dg}<\frac{e}{n}\cdot\frac{1}{1-0.00021214}<1.00022\,\frac{e}{n}\implies \frac{k}{dg}-\frac{e}{n}<\frac{2.1219e}{n\sqrt{n}}\,.\end{aligned}$$

Let m be the largest odd integer such that

$$\frac{p_m}{q_m}>\frac{e}{n}+\frac{2.1219e}{n\sqrt{n}}.$$

We have two possibilities depending on whether the inequality $\frac{p_{m+2}}{q_{m+2}}\geq\frac{k}{dg}$ is satisfied or not.

1. CASE: In the first case we assume that $\frac{p_{m+2}}{q_{m+2}}<\frac{k}{dg}$. We have

$$\left|\frac{e}{n}-\frac{k}{dg}\right|<\frac{2.1219e}{n\sqrt{n}}<\frac{2.1219}{G\sqrt{n}}=\frac{\frac{2.1219D^2g^2}{G}}{(dg)^2},$$

and from Theorem 1 we conclude that

$$\frac{k}{dg}=\frac{rp_{m+1}+sp_m}{rq_{m+1}+sq_m}\quad\text{or}\quad\frac{k}{dg}=\frac{sp_{m+2}-tp_{m+1}}{sq_{m+2}-tq_{m+1}},$$

where $m\geq -1$, and r,s and t are nonnegative integers satisfying inequalities $rs<4.2438\frac{D^2g^2}{G}$ and $st<4.2438\frac{D^2g^2}{G}$.

If we search for $\frac{k}{dg}$ among the fractions of the form $\frac{rp_{m+1}+sp_m}{rq_{m+1}+sq_m}$, we have the system

$$\begin{aligned}k&=rp_{m+1}+sp_m,\\ dg&=rq_{m+1}+sq_m\,.\end{aligned}$$

The determinant of this system is $p_{m+1}q_m-p_mq_{m+1}=-(-1)^{m+1}=-1$, and therefore, the system has positive integer solutions:

$$\begin{aligned}r&=dgp_m-kq_m,\\ s&=kq_{m+1}-dgp_{m+1}\,.\end{aligned}$$

If r and s are small, then they can be found by an exhaustive search. Let us find upper bounds for r and s. From [8, Theorem 9 and 13], we obtain

$$r=dgp_m-kq_m=dgq_m\left(\frac{p_m}{q_m}-\frac{k}{dg}\right)<dgq_m\left(\frac{p_m}{q_m}-\frac{e}{n}\right)<dgq_m\cdot\frac{1}{q_mq_{m+1}}=\frac{dg}{q_{m+1}}\,.$$

In the estimate for s we consider two possibilities. Assume first that

$$\frac{e}{n}-\frac{p_{m+1}}{q_{m+1}}>\frac{2.1219e}{n\sqrt{n}}.$$

Then

$$s = kq_{m+1} - dgp_{m+1} = dgq_{m+1}\left(\frac{k}{dg} - \frac{p_{m+1}}{q_{m+1}}\right) = dgq_{m+1}\left(\frac{k}{dg} - \frac{e}{n} + \frac{e}{n} - \frac{p_{m+1}}{q_{m+1}}\right)$$
$$< 2dgq_{m+1}\cdot\left(\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}}\right) < 2dgq_{m+1}\cdot\frac{1}{q_{m+1}q_{m+2}} = \frac{2dg}{q_{m+2}}\,.$$

Since

$$\frac{1}{q_{m+2}^2\,(a_{m+3}+2)} < \frac{p_{m+2}}{q_{m+2}} - \frac{e}{n} < \frac{2.1219e}{n\sqrt{n}} < \frac{2.1219}{G\sqrt{n}},$$

(see [8, Theorem 13]) we have

$$q_{m+2} > \frac{\sqrt{G}\,\sqrt[4]{n}}{\sqrt{2.1219\,(a_{m+3}+2)}}\,. \tag{9}$$

Putting all these estimates together, we obtain

$$r < \frac{dg}{q_{m+1}} < \frac{dg}{\frac{q_{m+2}}{a_{m+2}+1}} = \frac{dg\,(a_{m+2}+1)}{q_{m+2}} < \frac{dg\,(a_{m+2}+1)\sqrt{2.1219\,(a_{m+3}+2)}}{\sqrt{G}\,\sqrt[4]{n}}$$
$$< \sqrt{2.1219\,(a_{m+3}+2)}\,(a_{m+2}+1)\,\frac{Dg}{\sqrt{G}}\,,$$
$$s < \frac{2dg}{q_{m+2}} < \frac{2dg\sqrt{2.1219\,(a_{m+3}+2)}}{\sqrt{G}\,\sqrt[4]{n}} = 2\cdot\sqrt{2.1219\,(a_{m+3}+2)}\,\frac{Dg}{\sqrt{G}},$$

and finally

$$rs < 4.2438\,(a_{m+3}+2)\,(a_{m+2}+1)\,\frac{D^2g^2}{G}\,. \tag{10}$$

Assume now that $\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} \leq \frac{2.1219e}{n\sqrt{n}}$. Then, analogously to (9), we obtain

$$q_{m+1} > \frac{\sqrt{G}\,\sqrt[4]{n}}{\sqrt{2.1219\,(a_{m+2}+2)}} \qquad \text{and} \qquad r < \frac{dg}{q_{m+1}},$$

which imply

$$r < \frac{dg\sqrt{2.1219\,(a_{m+2}+2)}}{\sqrt{G}\,\sqrt[4]{n}} = \sqrt{2.1219\,(a_{m+2}+2)}\,\frac{Dg}{\sqrt{G}}\,,$$
$$s = dgq_{m+1}\left(\frac{k}{dg} - \frac{p_{m+1}}{q_{m+1}}\right) < dgq_{m+1}\left(\frac{p_m}{q_m} - \frac{p_{m+1}}{q_{m+1}}\right)$$
$$= dgq_{m+1}\cdot\frac{p_mq_{m+1} - p_{m+1}q_m}{q_mq_{m+1}} = dgq_{m+1}\cdot\frac{1}{q_mq_{m+1}} = \frac{dg}{q_m}$$
$$< \frac{dg}{\frac{q_{m+1}}{a_{m+1}+1}} = \frac{dg\,(a_{m+1}+1)}{q_{m+1}} < \frac{dg\,(a_{m+1}+1)\sqrt{2.1219\,(a_{m+2}+2)}}{\sqrt{G}\,\sqrt[4]{n}}$$
$$< \sqrt{2.1219\,(a_{m+2}+2)}\,(a_{m+1}+1)\,\frac{Dg}{\sqrt{G}}\,.$$

In this case we obtain

$$rs < 2.1219\,(a_{m+2}+2)\,(a_{m+1}+1)\,\frac{D^2g^2}{G}. \tag{11}$$

Inequalities (10) and (11) immediatelly give the bounds for the number of possible pairs (r,s). However, the bounds can be improved by combining them with the previous estimate $rs < 4.2428 \cdot \frac{D^2g^2}{G}$. This estimate and $r = a_{m+2}s - t < a_{m+2}s$ imply

$$r < \sqrt{4.2438a_{m+2}}\;\frac{Dg}{\sqrt{G}}.$$

Also, we have that $s \le s_1$, where $s_1 = \left\lfloor 2\cdot\sqrt{2.1219\,(a_{m+3}+2)}\;\frac{Dg}{\sqrt{G}}\right\rfloor$ if $\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} > \frac{2.1219e}{n\sqrt{n}}$, and $s_1 = \left\lfloor \sqrt{2.1219\,(a_{m+2}+2)}\,(a_{m+1}+1)\;\frac{Dg}{\sqrt{G}}\right\rfloor$ if $\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} \le \frac{2.1219e}{n\sqrt{n}}$.

Let $s_0 = \left\lfloor\sqrt{4.2438}\;\frac{Dg}{\sqrt{G}\sqrt{a_{m+2}}}\right\rfloor$. We have the following upper bound for the number of possible pairs (r,s):

$$\begin{aligned}
&a_{m+2}\;(1+2+3+\cdots+(s_0-1)) + 4.2438\,\tfrac{D^2g^2}{G}\left(\tfrac{1}{s_0}+\tfrac{1}{s_0+1}+\cdots+\tfrac{1}{s_1}\right)\\
&\quad< a_{m+2}\cdot\tfrac{s_0(s_0-1)}{2} + 4.2438\,\tfrac{D^2g^2}{G}\left(1+\int_{s_0}^{s_1}\tfrac{dx}{x}\right) < a_{m+2}\cdot\tfrac{s_0^2}{2} + 4.2438\,\tfrac{D^2g^2}{G}\left(1+\ln\tfrac{s_1}{s_0}\right)\\
&\quad< \tfrac{a_{m+2}}{2}\cdot 4.2438\,\tfrac{D^2g^2}{G\,a_{m+2}} + 4.2438\,\tfrac{D^2g^2}{G}\left(1+\ln\tfrac{s_1}{s_0}\right) = 4.2438\,\tfrac{D^2g^2}{G}\left(1.5+\ln\tfrac{s_1}{s_0}\right)\\
&\quad< 4.2438\,\tfrac{D^2g^2}{G}\;(1.5+\ln(0.7072\,\max(A,B)))\\
&\quad< 4.2438\,\tfrac{D^2g^2}{G}\;(1.1536+\ln(\max(A,B)))\,,
\end{aligned}$$

where

$$A = 2\sqrt{a_{m+2}\,(a_{m+3}+2)} \qquad\text{and}\qquad B = \sqrt{a_{m+2}\,(a_{m+2}+2)}\,(a_{m+1}+1)\ .$$

Let $P\,(a_i = q)$ be the probability that the partial quotient a_i, of the real number α, is equal to q, when α is chosen at random. Then we have the following formula [9, p. 368]

$$P\,(a_i = q) = \log_2\left(1+\frac{1}{(q+1)^2-1}\right). \tag{12}$$

We have that the success of this attack depends on the size of corresponding partial quotients a_{m+1}, a_{m+2} and a_{m+3}. From (12) we have that these partial quotients are usually small, but we can exclude the possibility that at least one of them is large.

We obtain the following experimental results (which are in good agreement with theoretical results which follow from (12), assuming that a_i are independent)

$$P\,(\max\{A,B\} \le 13) = 0.5135, \tag{13}$$

$$P\,(\max\{A,B\} \le 104) = 0.9002\,. \tag{14}$$

If we take 1000000 randomly chosen pairs of prime numbers p and q, such that $10^{10} < p,q < 10^{50}$, then we obtain the following results. In 50% cases we have $G = 2$, and in 90% cases we have $G \le 18$. By these results and (13), in 25% cases we have $G = 2$ and $\max\{A, B\} \le 13$, which imply that in 25% cases the upper bound for the number of possible pairs (r, s) is $31.5616D^2$. Also, in 81% cases we have $G \le 18$ and $\max\{A, B\} \le 104$. Thus, in 81% cases the upper bound for the number of possible pairs (r, s) is $442.8992D^2$.

We have the same upper bounds for the number of possible pairs (s, t).

2. CASE: We assume $\frac{p_{m+2}}{q_{m+2}} \ge \frac{k}{dg}$. In this case we have

$$\frac{k}{dg} = \frac{r' p_{m+3} + s' p_{m+2}}{r' q_{m+3} + s' q_{m+2}},$$

and similarly to the first case we have

$$\begin{aligned} r' &= dgp_{m+2} - kq_{m+2}, \\ s' &= kq_{m+3} - dgp_{m+3}\,. \end{aligned}$$

Now we have

$$\begin{aligned} s' &= dgq_{m+3}\left(\frac{k}{dg} - \frac{p_{m+3}}{q_{m+3}}\right) \le dgq_{m+3}\left(\frac{p_{m+2}}{q_{m+2}} - \frac{p_{m+3}}{q_{m+3}}\right) \\ &= dgq_{m+3}\cdot\frac{p_{m+2}q_{m+3} - p_{m+3}q_{m+2}}{q_{m+2}q_{m+3}} = \frac{dg}{q_{m+2}} \\ &< \frac{dg}{\frac{\sqrt{G}\,\sqrt[4]{n}}{\sqrt{2.1219(a_{m+3}+2)}}} < \frac{dg\sqrt{2.1219\,(a_{m+3}+2)}}{\sqrt{G}\,\sqrt[4]{n}} \\ &= \sqrt{2.1219\,(a_{m+3}+2)}\;\frac{Dg}{\sqrt{G}}, \\ r' &= dgq_{m+2}\left(\frac{p_{m+2}}{q_{m+2}} - \frac{k}{dg}\right) < dgq_{m+2}\left(\frac{p_{m+2}}{q_{m+2}} - \frac{e}{n} + \frac{e}{n} - \frac{k}{dg}\right) \\ &< dgq_{m+2}\cdot\frac{0.1219e}{n\sqrt{n}} < dgq_{m+2}\cdot 0.061\cdot\frac{2e}{n\sqrt{n}} \\ &< 0.061dgq_{m+2}\left(\frac{p_{m+2}}{q_{m+2}} - \frac{e}{n}\right) < 0.061dgq_{m+2}\frac{1}{q_{m+2}q_{m+3}} \\ &= \frac{0.061dg}{q_{m+3}} = \frac{0.061dg}{a_{m+3}q_{m+2} + q_{m+1}} < \frac{0.061dg}{a_{m+3}q_{m+2}} < \frac{0.061dg}{a_{m+3}\cdot\frac{\sqrt{G}\,\sqrt[4]{n}}{\sqrt{2.1219(a_{m+3}+2)}}} \\ &= \frac{0.061\sqrt{2.1219\,(a_{m+3}+2)}}{a_{m+3}}\cdot\frac{Dg}{\sqrt{G}} < 0.1540\cdot\frac{Dg}{\sqrt{G}}\,. \end{aligned}$$

Hence, we have the following upper bound for the number of possible pairs (r', s')

$$r's' < \frac{0.061\cdot 2.1219\,(a_{m+3}+2)}{a_{m+3}}\cdot\frac{D^2g^2}{G} < 0.3884\,\frac{D^2g^2}{G}\,.$$

We will now consider how one could test whether a guess of k and dg is correct. Since $g < k$, from (8) we have that a guess of $(p-1)(q-1)$ is $\left\lfloor \frac{e\cdot dg}{k} \right\rfloor$, while a guess of g is $edg \bmod k$. The guess of $(p-1)(q-1)$ can be used to create a guess of $\frac{p+q}{2}$ using the following identity

$$\frac{p+q}{2} = \frac{n-(p-1)(q-1)+1}{2}\,.$$

If the guess of $\frac{p+q}{2}$ is not an integer, then the guess of k and dg is wrong. The guess of $\frac{p+q}{2}$ can be used to create a guess of $\left(\frac{q-p}{2}\right)^2$ using the following identity

$$\left(\frac{q-p}{2}\right)^2 = \left(\frac{p+q}{2}\right)^2 - n\,. \tag{15}$$

If the guess of $\left(\frac{q-p}{2}\right)^2$ is a perfect square, then the original guess of k and dg is correct. The secret key d can be found by dividing dg by g. Recall that g is the remainder on division of edg by k. We can also recover p and q easily from $\frac{p+q}{2}$ and $\frac{q-p}{2}$, by

$$p = \frac{p+q}{2} - \frac{q-p}{2} \qquad \text{and} \qquad q = \frac{p+q}{2} + \frac{q-p}{2}\,.$$

Example 1. *Let us take 25-digits number* $n = 1338871137782389210296931$ *and* $e = 1061543036400634755716333$. *The first 16 partial quotients of the continued fraction expansion of* e/n *are*

$$[0, 12, 1, 1, 1, 1, 2, 1, 1, 1, 1, 982, 7, 1, 4, 18, \ldots]\,,$$

and the first 14 convergents are

$$0, \frac{1}{12}, \frac{1}{13}, \frac{2}{25}, \frac{3}{38}, \frac{5}{63}, \frac{13}{164}, \frac{18}{227}, \frac{31}{391}, \frac{49}{618}, \frac{80}{1009}, \frac{78609}{991456}, \frac{550343}{6941201}, \frac{628952}{7932657}, \ldots\,.$$

We find that

$$\frac{78609}{991456} < \frac{e}{n} + \frac{2.1219e}{n\sqrt{n}} < \frac{49}{618}\,,$$

and we have $m = 9$. *We are searching for the rational number* k/dg *among the numbers*

$$\frac{80r + 49s}{1009r + 618s}, \qquad \frac{78609s - 80t}{991456s - 1009t} \qquad or \qquad \frac{550343r' + 78609s'}{6941201r' + 991456s'}\,.$$

By applying the above described test, we find that $s = 209$ *and* $t = 2$ *gives the correct value for secret key* d *(i.e. for* k *and* dg*). We have* $d = 34535381$, *and* $p = 936938270533$, $q = 1428985430407$.

If we compare these numbers s *and* t *with the numbers* r *and* s *obtained by an application of the Verheul and van Tilborg attack to the same problem, we have the same number* $s = 209$, *but the other number* $r = 205236$ *is much greater than the number* $t = 2$.

Example 2. *Let* $n = 881542675172451959659$. *Among* 1000000 *trials with a randomly chosen private key* d, *such that* $\frac{1}{3}n^{0.25} < d < 10^9 \cdot \frac{1}{3}n^{0.25}$ *we have the following results. In* 991847 (99.18%) *trials we have that* $\frac{p_{m+2}}{q_{m+2}} < \frac{k}{dg}$. *The value of*

$\min\{rs, st\}$ *is equal to* rs *in* 491974 (49.20%) *cases, and it is equal to* st *in* 499873 (49.99%) *cases. The maximal value of these minimums is* 7872119858569929382 *and it is attained for* $d = 56718771847943$. *The average value of* $\min\{rs, st\}$ *is* 838805216031098771 3.27. *The maximal value of* $\frac{G\cdot\min\{rs,st\}}{D^2g^2}$ *is* 4.0363 *and it is attained for* $d = 56718771847943$. *The average value of these minimums for* d *in the given interval is* 0.8455.

In 8153 (0.82%) *trials we have that* $\frac{p_{m+2}}{q_{m+2}} \geq \frac{k}{dg}$. *The maximal value of products* $r's'$ *is* 1081631134948304523, *and it is attained for* $d = 38407030686079$. *The average value of these products is* 5611757083137645.76. *The maximal value of* $\frac{Gr's'}{D^2g^2}$ *is* 0.0762 *and it is attained for* $d = 12320751623657$. *The average value of these products is* 0.0193.

4.2. Case $S(n) = \mathrm{lcm}\,(p+1, q+1)$

Analogously to the previous section we have

$$\frac{1.9997e}{n\sqrt{n}} < \frac{e}{n} - \frac{k}{dg} < \frac{2.1216e}{n\sqrt{n}}\,.$$

Let m be the largest even integer such that

$$\frac{p_m}{q_m} < \frac{e}{n} - \frac{2.1216e}{n\sqrt{n}}.$$

As in Section 4.1, we have two possibilities depending on whether the inequality $\frac{p_{m+2}}{q_{m+2}} \leq \frac{k}{dg}$ is satisfied or not. In the first case we can assume that $\frac{p_{m+2}}{q_{m+2}} > \frac{k}{dg}$. If $\frac{p_{m+1}}{q_{m+1}} - \frac{e}{n} > \frac{2.1216e}{n\sqrt{n}}$, then we have

$$\begin{aligned} r &< \sqrt{2.1216\,(a_{m+3}+2)}\,(a_{m+2}+1)\,\frac{Dg}{\sqrt{G}}, \\ s &< 2\cdot\sqrt{2.1216\,(a_{m+3}+2)}\,\frac{Dg}{\sqrt{G}}, \\ rs &< 4.2432\,(a_{m+3}+2)\,(a_{m+2}+1)\,\frac{D^2g^2}{G}\,. \end{aligned}$$

If $\frac{p_{m+1}}{q_{m+1}} - \frac{e}{n} \leq \frac{2.1216e}{n\sqrt{n}}$, then we have

$$\begin{aligned} r &< \sqrt{2.1216\,(a_{m+2}+2)}\,\frac{Dg}{\sqrt{G}}, \\ s &< \sqrt{2.1216\,(a_{m+2}+2)}\,(a_{m+1}+1)\,\frac{Dg}{\sqrt{G}}, \\ rs &< 2.1216\,(a_{m+2}+2)\,(a_{m+1}+1)\,\frac{D^2g^2}{G}\,. \end{aligned}$$

Thus, we obtain the following upper bound for the number of possible pairs (r, s), and also (s, t)

$$4.2432\,\frac{D^2g^2}{G}\,\left(1.1536 + \ln\left(\max\left(A, B\right)\right)\right).$$

In the second case we assume that $\frac{p_{m+2}}{q_{m+2}} \leq \frac{k}{dg}$ and obtain

$$\begin{aligned} s' &< \sqrt{2.1216\,(a_{m+3}+2)}\;\frac{Dg}{\sqrt{G}}, \\ r' &< \frac{0.061\sqrt{2.1216\,(a_{m+3}+2)}}{a_{m+3}}\cdot\frac{Dg}{\sqrt{G}} < 0.1539\cdot\frac{Dg}{\sqrt{G}}\,. \end{aligned}$$

The upper bound for the number of the possible pairs (r', s') is

$$r's' < 0.3883\,\frac{D^2g^2}{G}\,.$$

The guess of $(p+1)\,(q+1)$ is $\left\lfloor \frac{e\cdot dg}{k} \right\rfloor$, and of g is edg mod k. We can determine p and q from (15) and the identity

$$\frac{p+q}{2} = \frac{(p+1)\,(q+1)-n-1}{2}\,.$$

Example 3. *Let us take again* $n = 133887113778238921029 6931$ *and now* $e = 2232010317703392588027 23$. *In this case we have* $m = 2, s = 947366288,\ \ t = 207$ *(and* $r = 5684197521$*). We obtain the fraction* k/dg *in the form*

$$\frac{k}{dg} = \frac{3997\cdot 947366288 - 666\cdot 207}{23976\cdot 947366288 - 3995\cdot 207}\,.$$

Finally, we obtain $d = 22714053294123$ *and* $p = 936938270533, q = 1428985430407$.

4.3. Case $S\,(n) = \mathrm{lcm}\,(p+1, q-1)$

In this case we have

$$\frac{0.9999e}{n\,(n+0.9999)} < \frac{e}{n} - \frac{k}{dg} < \frac{0.7072e}{n\sqrt{n}}\,.$$

Let m be the largest even integer such that

$$\frac{p_m}{q_m} < \frac{e}{n} - \frac{0.7072e}{n\sqrt{n}}.$$

Let $\frac{p_{m+2}}{q_{m+2}} > \frac{k}{dg}$ and assume that $\frac{p_{m+1}}{q_{m+1}} - \frac{e}{n} > \frac{0.7072e}{n\sqrt{n}}$. We obtain

$$\begin{aligned} r &< \sqrt{0.7072\,(a_{m+3}+2)}\,(a_{m+2}+1)\,\frac{Dg}{\sqrt{G}}, \\ s &< 2\cdot\sqrt{0.7072\,(a_{m+3}+2)}\;\frac{Dg}{\sqrt{G}}, \\ rs &< 1.4144\,(a_{m+3}+2)\,(a_{m+2}+1)\,\frac{D^2g^2}{G}\,. \end{aligned}$$

If we assume $\frac{p_{m+1}}{q_{m+1}} - \frac{e}{n} \le \frac{0.7072e}{n\sqrt{n}}$, then we have

$$\begin{aligned} r &< \sqrt{0.7072\,(a_{m+2}+2)}\,\frac{Dg}{\sqrt{G}}, \\ s &< \sqrt{0.7072\,(a_{m+2}+2)\,(a_{m+1}+1)}\,\frac{Dg}{\sqrt{G}}, \\ rs &< 0.7072\,(a_{m+2}+2)\,(a_{m+1}+1)\,\frac{D^2g^2}{G}\,. \end{aligned}$$

The upper bound for the number of possible pairs (r, s), and also (s, t), is

$$1.4144\,\frac{D^2g^2}{G}\,\left(1.1536 + \ln\left(\max\left(A, B\right)\right)\right)\,.$$

Let $\frac{p_{m+2}}{q_{m+2}} \le \frac{k}{dg}$. In this case we have

$$\begin{aligned} s' &< \sqrt{0.7072\,(a_{m+3}+2)}\,\frac{Dg}{\sqrt{G}}, \\ r' &< 1.4566 \cdot \frac{Dg}{\sqrt{G}}\,, \end{aligned}$$

and we obtain the following upper bound for the number of possible pairs (r', s')

$$r's' < 0.7072 \cdot \frac{D^2g^2}{G}\,.$$

The guess of $(p+1)(q-1)$ is $\left\lfloor \frac{e \cdot dg}{k} \right\rfloor$, and of g is edg mod k. Factors p and q can be obtained from

$$\frac{q-p}{2} = \frac{(p+1)(q-1) - n + 1}{2}, \tag{16}$$

$$\left(\frac{p+q}{2}\right)^2 = \left(\frac{q-p}{2}\right)^2 + n\,. \tag{17}$$

Example 4. *Let us take again* $n = 1338871137782389210296931$ *and now* $e = 1483381188766593912 15397$. *In this case we have* $m = 4, s = 1009345869$, $t = 256$ *(and* $r = 1009345613$*). Thus, we obtain the fraction* k/dg *in the form*

$$\frac{k}{dg} = \frac{75989 \cdot 1009345869 - 75834 \cdot 256}{685862 \cdot 1009345869 - 684463 \cdot 256}\,.$$

Finally, we obtain $d = 346135900590775$ *and* $p = 936938270533, q = 1428985430407$.

4.4. Case $S(n) = \mathrm{lcm}(p-1, q+1)$

In this case we have

$$\frac{1.9999e}{n\,(n-1.9999)} < \frac{k}{dg} - \frac{e}{n} < \frac{0.7074e}{n\sqrt{n}}\,.$$

Let m be the largest odd integer such that

$$\frac{p_m}{q_m} > \frac{e}{n} + \frac{0.7074e}{n\sqrt{n}}.$$

Let $\frac{p_{m+2}}{q_{m+2}} < \frac{k}{dg}$ and assume that $\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} > \frac{0.7074e}{n\sqrt{n}}$. Then we have

$$\begin{aligned} r &< \sqrt{0.7074\,(a_{m+3}+2)}\,(a_{m+2}+1)\,\frac{Dg}{\sqrt{G}}\,, \\ s &< 2\cdot\sqrt{0.7074\,(a_{m+3}+2)}\,\,\frac{Dg}{\sqrt{G}}\,, \\ rs &< 1.4148\,(a_{m+3}+2)\,(a_{m+2}+1)\,\frac{D^2g^2}{G}. \end{aligned}$$

If we assume $\frac{e}{n} - \frac{p_{m+1}}{q_{m+1}} \leq \frac{0.7074e}{n\sqrt{n}}$, then we have

$$\begin{aligned} r &< \sqrt{0.7074\,(a_{m+2}+2)}\,\,\frac{Dg}{\sqrt{G}}\,, \\ s &< \sqrt{0.7074\,(a_{m+2}+2)}\,(a_{m+1}+1)\,\frac{Dg}{\sqrt{G}}\,, \\ rs &< 0.7074\,(a_{m+2}+2)\,(a_{m+1}+1)\,\frac{D^2g^2}{G}. \end{aligned}$$

In this case we obtain the following upper bound for the number of possible pairs (r,s), and also (s,t), $1.4148\,\frac{D^2g^2}{G}\,\left(1.1536 + \ln\left(\max\left(A,B\right)\right)\right)$.

If we have $\frac{p_{m+2}}{q_{m+2}} \geq \frac{k}{dg}$, then we obtain

$$\begin{aligned} s' &< \sqrt{0.7074\,(a_{m+3}+2)}\,\,\frac{Dg}{\sqrt{G}}, \\ r' &< 1.4566\cdot\frac{Dg}{\sqrt{G}}\,. \end{aligned}$$

The upper bound for the number of possible pairs (r', s') is

$$r's' < 0.7074\,\frac{D^2g^2}{G}\,.$$

The guess of $(p-1)(q+1)$ is $\left\lfloor \frac{e\cdot dg}{k} \right\rfloor$, and of g is $edg \bmod k$. Factors p and q can be obtained from (17) and

$$\frac{q-p}{2} = \frac{n-(p-1)(q+1)-1}{2}\,.$$

Example 5. *Let us take the same $n = 133887113778238921029693 1$ and now $e = 293598101817010770384145$. In this case we have $m = 17, s = 46041557$, $t = 120$ (and $r = 138124551$) and we obtain the fraction k/dg in the form*

$$\frac{k}{dg} = \frac{343149\cdot 46041557 - 89285\cdot 120}{1564834\cdot 46041557 - 407159\cdot 120}\,.$$

Finally, we obtain $d = 36023672473729$ and $p = 936938270533$, $q = 1428985430407$.

Example 6. *Let* $n = 881542675172451959659$*. Among* 1000000 *trials with a randomly chosen private key* d*, such that* $\frac{1}{3}n^{0.25} < d < 10^9 \cdot \frac{1}{3}n^{0.25}$*, we compare the obtained results in three cases, depending on function* $S(n)$*. We consider function* S *in the form* $S(n) = \operatorname{lcm}(p-1, q+1)$*,* $\operatorname{lcm}(p-1, q+1)$ *and* $\operatorname{lcm}(p-1, q+1)$*, respectively.*

In 990587 (99.06%)*,* 893373 (89.34%) *and* 882391 (88.24%) *trials, resp., we obtained* k *and* dg *with pairs* (r, s) *and* (s, t)*. More precisely,* $\min\{rs, st\}$ *is equal to* rs *in* 488275 (48.83%)*,* 393932 (39.39%) *and* 383390 (38.34%) *trials, and it is equal to* st *in* 502312 (50.23%)*,* 499441 (49.94%) *and* 499001 (49.90%) *trials. The maximal values of these minimums are*

$$721090380565428735 \quad (d = 342804871054489)\,,$$
$$125268491259184839 \quad (d = 334161510529429)$$

and

$$326408359472540736 \quad (d = 56974579771127)\,.$$

The average values of these minimums are

1425002034008237123.16, 705703219014797180.45 *and* 15886594335277959.27.

The maximal values of $\frac{G \cdot \min\{rs, st\}}{D^2 g^2}$ *are*

$$4.0330 \quad (d = 299225532498339)\,,$$
$$0.8205 \quad (d = 329534695410043)$$

and

$$0.7977 \quad (d = 54342302187019)\,,$$

and the average values are 0.8561*,* 0.1899 *and* 0.1841*.*

In 9413 (0.94%)*,* 106637 (10.66%) *and* 117609 (11.76%) *trials we obtained* k *and* dg *with pairs* (r', s')*. The maximal values of products* $r's'$ *are*

$$1063899527763072894 \quad (d = 300078163615589)\,,$$
$$1241778639590097406 \quad (d = 104182591660513)$$

and

$$86705428719975975 \quad (d = 55869596982065)\,,$$

and the average values are 1425002034008237123.16*,* 705703219014797180.45 *and* 15886594335277959.27*. The maximal values of* $\frac{Gr's'}{D^2 g^2}$ *are*

$$0.0708 \quad (d = 49908237142041)\,,$$
$$0.2038 \quad (d = 278995224797287)$$

and

$$0.2218 \quad (d = 23630365395965)\,,$$

and the average values of these products are 0.0208*,* 0.0486 *and* 0.0500*.*

Note that the LUC cryptosystem with a 1024-bit modulus n is factoring–secure. In this case, Pinch [12] showed that the LUC cryptosystem is insecure for a 256-bit d. We have implemented the attack described in this paper in the computer algebra system PARI/GP (on a 3.0GHz – Pentium under Windows XP). It works efficiently for $D \leq 2^{14}$. More precisely, an implementation of this attack needs on average around one hour for $D \leq 2^{13}$ and around 5 hours for $D \leq 2^{14}$. Thus, we conclude that our attack shows that the LUC cryptosystem, with a 1024-bit modulus n, is insecure for a 270–bit secret key d.

References

[1] D. Bleichenbacher, W. Bosma, A. K. Lenstra, *Some Remarks on Lucas–based Cryptosystems*, Advances in Cryptology - Crypto '95, Lecture Notes in Comput. Sci. **963**(1995), 386-396.

[2] J. Blömer, A. May, *Low secret exponent RSA revisited*, Cryptography and Lattices - Proceedings of CaLC 2001, Lecture Notes in Comput. Sci. **2146**(2001), 4-19.

[3] D. Boneh, G. Durfee, *Cryptanalysis of RSA with private key d less than* $N^{0.292}$, Advances in Cryptology - Proceedings of Eurocrypt '99, Lecture Notes in Comput. Sci. **1952**(1999), 1-11.

[4] D. Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, J. Cryptology **10**(1997), 233-260.

[5] A. Dujella, *Continued fractions and RSA with small secret exponent*, Tatra Mt. Math. Publ. **29**(2004), 101-112.

[6] A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[7] B. Ibrahimpašić, *Cryptanalysis of KMOV cryptosystem with short secret exponent*, in: *Proceedings of the* 19^{th} *Central European Conference on Information and Intelligent Systems*, (B. Aurer, M. Bača and K. Rabuzin, Eds.), Varaždin, 2008, 407-414.

[8] A. Ya. Khinchin, *Continued Fractions.* Dover, New York, 1997.

[9] D. E. Knuth, *The Art of Computer Programming*, Vol. 2, Seminumerical Algorithms, 3rd ed, Addison–Wesley, Reading, 1997.

[10] K. Koyama, U. M. Maurer, T. Okamoto, S. A. Vanstone, *New public–key schemes based on elliptic curves over the ring* $\mathbb{Z}_n$, Advances in Cryptology - Crypto '91, Lecture Notes in Computer Science, Springer–Verlag, 1991, 252-266.

[11] D. H. Lehmer, *An extended theory of Lucas functions*, Annals of Math. **31**(1930), 419-448.

[12] R. G. E. Pinch, *Extending the Wiener attack to RSA–type cryptosystems*, Electronics Letters **31**(1995), 1736-1738.

[13] R. L. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public–key cryptosystems*, Communications of the ACM **21**(1978), 120-126.

[14] P. J. Smith, G. J. J. Lennon, *LUC: a new public–key cryptosystem*, Ninth IFIP Symposium on Computer Science Security, Elsevier Science Publishers (1993), 103-117.

[15] E. R. Verheul, H. C. A. Van Tilborg, *Cryptanalysis of 'less short' RSA secret exponents*, Appl. Algebra Engrg. Comm. Computing **8**(1997), 425-435.

[16] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Inform. Theory **36**(1990), 553-558.

[17] R. T. Worley, *Estimating* $|\alpha - p/q|$, Austral. Math. Soc. Ser. A **31**(1981), 202-206.