Cryptanalysis of KMOV cryptosystem with short secret exponent

Bernadin Ibrahimpašić
Pedagogical Faculty
University of Bihać
Džanića mahala 36, 77000 Bihać, Bosnia and Herzegovina
bernadin@bih.net.ba

Abstract. *In this paper we analyze the KMOV public key cryptosystem, which is an elliptic curve based analogue to RSA. We extend the Dujella variant of well-known Wiener attack on KMOV cryptosystem*

Keywords. KMOV, Cryptanalysis, Continued fractions, Diophantine approximations

1 Introduction

In 1976, Diffie and Hellman [1] proposed the first public–key exchange protocol for exchanging secret keys over insecure channels. This protocol is not a public–key cryptosystem, but it is the basis for the cryptosystems. In 1978, Rivest, Shamir and Adleman [10] proposed the first practical public–key cryptosystem, now widely known as the RSA public–key cryptosystem. Its security is based on the assumption that it is not so difficult to find two large prime numbers, but it is very difficult to factor a large composite into its prime factorization form. 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 1985, Koblitz [6] and Miller [8] independently proposed new public–key cryptosystems based on elliptic curves. These cryptosystems rely on the difficulty to solve the discrete logarithm problem for elliptic curves.

In 1991, Koyama, Maurer, Okamoto and Vanstone [7] proposed another kind of elliptic curve based cryptosystems. Their schemes are based on the difficulty of factoring large numbers and are similar to RSA. The most practical of these schemes (Type 1) is generally called the KMOV public–key cryptosystem, according to the first letters of the author's names.

A well–known attack on RSA with small secret exponent d, which is called the Wiener attack, was proposed by Wiener [13] in 1990. He showed that using continued fractions, one can efficiently recover the secret exponent d from public key (n, e) as long as $d < n^{0.25}$. In this case d is the denominator of some convergent p_m/q_m of the continued fraction expansion of e/n.

In 1997, Verheul and van Tilborg [11] extended the boundary of the Wiener attack on RSA. They propose a technique to raise the security 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 exponent d are of the form $d = rq_{m+1} + sq_m$, for some positive integers r and s.

In 2004, Dujella [2] described a modification of the Verheul and van Tilborg variant of the Wiener attack on RSA. Dujella's modifications of this attack is based on the Worley result on Diophantine approximations [14] of the form $|\alpha - a/b| < c/b^2$, for a positive real number c. 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 [9] extended the Wiener attack to KMOV cryptosystem.

Here we extend the Dujella variant of the Wiener attack to KMOV cryptosystem. We describe an algorithm for finding secret key d of the form $d = rq_{m+1} \pm sq_m$, for some nonnegative integers r and s. Using results on connection between continued fractions and rational approximations of the form $|\alpha - a/b| < c/b^2$, for a positive integer c, from Dujella and Ibrahimpašić [4] and above mentioned results on Diophantine approximations [2, 14], we derive bounds for r and s.

2 Elliptic curve over the ring $\mathbf{Z}_n$

Elliptic curves are described by the set of solutions to certain equations in two variables. We begin by looking briefly at elliptic curves [12, 3]

Let K be a field of characteristic $\neq 2, 3$ $(1+1 \neq 0$ and $1+1+1 \neq 0$ in $K)$, and let $x^3 + ax + b$ (where $a, b \in K$) be a cubic polynomial with no multiple roots $\left(4a^3 + 27b^3 \neq 0\right)$. An *elliptic curve* $E(a, b)$ *over* K is the set of points $(x, y) \in K \times K$ which satisfy the equation

$$y^2 = x^3 + ax + b,$$

together with a single element denoted $\mathcal{O}$ and called the *point at infinity*. We will mainly be interested in elliptic curves $E_p(a, b)$ over the finite field $\mathbf{F}_p$ with p elements, for some prime p. The fact that addition operation on the points of an elliptic curve can be defined that elliptic curve is an abelian group, makes elliptic curves interesting in cryptography. This addition operation is described in the following.

Let E be an elliptic curve, and let P and Q be two points on E. We define the negative of P and the sum $P + Q$ according to the following rules. If $P = \mathcal{O}$, then we define $-P = \mathcal{O}$ and $P+Q = Q$ (i.e. $\mathcal{O}$ is the neutral element of the group of points). If $P = (x, y)$, then $-P = (x, -y)$. Let $(x_1, y_1), (x_2, y_2)$ and (x_3, y_3) denote the coordinates of P, Q and $P+Q$, respectively. The coordinates (x_3, y_3) may be computed by

$$P_1 + P_2 = \begin{cases} \mathcal{O} & , \; x_1 = x_2 \;\&\; y_1 = -y_2 \\ (x_3, y_3) & , \; \text{otherwise} \end{cases} \tag{1}$$

where

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda (x_1 - x_3) - y_1 \end{aligned}$$

and

$$\lambda = \begin{cases} \frac{3x_1^2 + a}{2y_1} & , \; P_1 = P_2 \\ \frac{y_2 - y_1}{x_2 - x_1} & , \; \text{otherwise.} \end{cases} \tag{2}$$

All computations are in the field over which E is defined. In particular, when the field is $\mathbf{F}_p$, all computations are modulo p.

Let $\#E_p(a, b)$ denote the order (i.e. the number of points) of the elliptic curve $E_p(a, b)$. It well-known that $p+1-2\sqrt{p} \leq \#E_p(a, b) \leq p+1+2\sqrt{p}$. There exists a polynomial-time algorithm for computing the order of an elliptic curve, but this algorithm is quite impractical for large p. It is known that $E_p(a, b)$ is either cyclic or the product of two cyclic groups. In the latter case, $E_p(a, b) \cong \mathbf{Z}_{N_1} \times \mathbf{Z}_{N_2}$, where $N_1 \cdot N_2 = \#E_p(a, b)$, where N_2 divides N_1 and where N_2 also divides $p - 1$. For some special classes of elliptic curves, the order and group structure is easily determined. If p an odd prime satisfying $p \equiv 2 \pmod 3$, then for $0 < b < p$, elliptic curve $E_p(0, b)$ is a cyclic group of order $p+1$ [7].

We now consider elliptic curves over the ring $\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$, where n denote the product of two large distinct primes p and q. Like the definition over the field $\mathbf{F}_p$, an elliptic curve $E_n(a, b)$ over the ring $\mathbf{Z}_n$ is the set of points $(x, y) \in \mathbf{Z}_n \times \mathbf{Z}_n$ satisfying the equation $y^2 = x^3 + ax + b \pmod n$ together with the point $\mathcal{O}$. An addition operation on $E_n(a, b)$ can be defined in the same way as the addition operation on $E_p(a, b)$, simply by replacing computations in $\mathbf{F}_p$ by computations in $\mathbf{Z}_n$, where all computations are modulo n. A rational number a/b in (2) must be treated as ab^{-1} where $b^{-1}b = 1 \pmod n$. However, two problems occur. The first problem is that because the computation of λ in (2) requires a division which in a ring is defined only when the divisor is a unit, the addition operation on $E_n(a, b)$ is not always defined. The second problem, which is related to the first is that $E_n(a, b)$ is not a group. It would therefore seem impossible to base a cryptographic system on $E_n(a, b)$. The authors of KMOV cryptosystem [7] presented a natural solution to these problems. By Chinese Remainder Theorem, every element on $E_n(a, b)$ can be represented uniquely as a pair of points, one on $E_p(a, b)$ and other on $E_q(a, b)$. In this way we have that $E_n(a, b)$ is isomorphic to $E_p(a, b) \oplus E_q(a, b)$. In practice is very unlikely that the addition of two points on $E_n(a, b)$ is undefined, where $n = pq$ for large p and q. The probability of finding two points such that their sum is undefined is the same than finding the two prime factor of n. The second problem, that

$E_n(a,b)$ is not a group, can be solved by the following statement which can be easily obtained from the Chinese Remainder Theorem. Let $E_n(a,b)$ be an elliptic curve such that $\gcd(4a^3+27b^2,n)=1$. If $N_n = \mathrm{lcm}(\#E_p(a,b), \#E_q(a,b))$, then

$$\forall P \in E_n(a,b), \forall k \in \mathbf{Z} \ : \ (kN_n+1)P = P. \quad (3)$$

We should note that it is possible to define an elliptic curve over a ring so that the resulting structure is a group, but for our purposes, this is unnecessary.

Example 1 Let $E_{35}(10,18)$ the elliptic curve $y^2 = x^3+10x+18$ over the ring $\mathbf{Z}_{35}$, and let $P=(x_1,y_1)=(1,8)$ and $Q=(x_2,y_2)=(23,5)$ be two points on E. We have:

Case 1: $P+Q$
$y_2 - y_1 = 5-8 = -3 = 32 \bmod 35$
$x_2 - x_1 = 23-1 = 22 \bmod 35$
$22^{-1} = 8 \bmod 35 \quad (22 \cdot 8 = 176 = 1 \bmod 35)$
$\lambda = 32 \cdot 8 = 256 = 11 \bmod 35$
$x_3 = 11^2 - 1 - 23 = 97 = 27 \bmod 35$
$y_3 = 11 \cdot (1-27) - 8 = -294 = 21 \bmod 35$

$$P+Q=(27,21)$$

Case 2: $P+P=2P$
$3x_1^2 + a = 3 \cdot 1^2 + 10 = 13 \bmod 35$
$2y_1 = 2 \cdot 8 = 16 \bmod 35$
$16^{-1} = 11 \bmod 35 \quad (16 \cdot 11 = 176 = 1 \bmod 35)$
$\lambda = 13 \cdot 11 = 143 = 3 \bmod 35$
$x_3 = 3^2 - 2 \cdot 1 = 7 \bmod 35$
$y_3 = 3 \cdot (1-7) - 8 = -26 = 9 \bmod 35$

$$2P=(7,9)$$

3 KMOV cryptosystem

Koyama, Maurer, Okamoto and Vanstone [7] proposed public key cryptosystem which is an elliptic curve based analogue to RSA. The authors propose using the elliptic curve $E_n(0,b)$ with equation $y^2=x^3+b$ modulo $n=pq$ where p and q are both congruent to 2 mod 3. In this case, the order $\#E_p(0,b)$ is $p+1$ and $\#E_q(0,b)$ is $q+1$.

Alice want to send a message M to Bob. They do the following.

1. Bob chooses two distinct large primes p and q with $p \equiv q \equiv 2 \pmod 3$ and computes $n=pq$.
2. Bob chooses integer e which is relatively prime to $\mathrm{lcm}(p+1,q+1)$.
3. Bob computes private key number d
$$ed \equiv 1 \pmod{\mathrm{lcm}(p+1,q+1)}.$$
4. Bob makes n and e public and he keeps d, p and q private.
5. Alice represents her message as a pair of integers $(m_1,m_2) \pmod n$. She regards (m_1,m_2) as a point M on the elliptic curve $E_n(0,b)$ given by
$$y^2 = x^3 + b \bmod n,$$
where $b = m_2^2 - m_1^3 \bmod n$ (she does not need to compute b).
6. Alice adds M to itself e times on E to obtain $C=(c_1,c_2)=eM$. She sends C to Bob.
7. Bob computes $M=dC$ on E to obtain M.

Note that the formulas for the addition law on $E_n(0,b)$ never use the value of b. Therefore, Bob never need to compute it, but he can compute it, if he wants as $b=c_2^2-c_1^3$.

Let's verify that encryption and decryption are inverse operations. Since

$$ed \equiv 1 \pmod{\mathrm{lcm}(p+1,q+1)},$$

we have that

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

for some positive integer K. Then, from (3) we have

$$dC = deM = (K \cdot \mathrm{lcm}(p+1,q+1)+1)M = M,$$

as desired.

The following algorithm implements the idea of repeated doubling and addition for computing eP (and similar for computing dP). This algorithm will compute the point $eP \bmod n$, where e is positive integer and $P=(x,y)$ is initial point on an elliptic curve $E_n(a,b)$: $y^2=x^3+ax+b$ over the ring $\mathbf{Z}_n$. The result point is $eP=(x_t,y_t)$.

Write e in the following binary expansion form $e = e_{s-1}e_{s-2}\ldots e_1e_0$.

```
$(x_t, y_t) \leftarrow (x, y)$
for $i$ from $s-2$ down to 0 do
    $m_1 \leftarrow 3x_t^2 + a \bmod n$
    $m_2 \leftarrow 2y_t \bmod n$
    $M \leftarrow m_1/m_2 \bmod n$
    $x_0 \leftarrow M^2 - 2x_t \bmod n$
    $y_0 \leftarrow M(x_t - x_0) - y_t \bmod n$
    $x_t \leftarrow x_0$
    $y_t \leftarrow y_0$
    if $e_i = 1$ then
                $m_1 \leftarrow y_t - y \bmod n$
                $m_2 \leftarrow x_t - x \bmod n$
                $M \leftarrow m_1/m_2 \bmod n$
                $x_t \leftarrow M^2 - x_t - x \bmod n$
                $y_t \leftarrow M(x_t - x_0) - y_t \bmod n$
                $x_t \leftarrow x_0$
                $y_t \leftarrow y_0$
print $(x_t, y_t)$
```

Example 2 Alice want to send a message to Bob. Bob chooses two distinct primes $p = 23$ and $q = 29$ and computes $n = pq = 667$. He chooses integer $e = 13$ with $\gcd(e, n) = 1$, and computes secret exponent $d = 37$ with $ed \equiv 1 \pmod{120}$ where $120 = \operatorname{lcm}(p+1, q+1)$. Bob makes $n = 667$ and $e = 13$ public.

Alice want to send the message $M = (1, 27)$ to Bob, where M is an point on an elliptic curve $E_{667}(0, 61) : \ y^2 = x^3 + 61$ over the ring $\mathbf{Z}_{667}$.

Alice adds M to itself $e = 13$ times on E_{667} to obtain $C = (c_1, c_2) = 13M$. She computes eM with the mentioned algorithm.

$$e = 13 = 1101_2 = e_3e_2e_1e_0$$

$$\begin{aligned} e_3 = 1 : \quad & (x_t, y_t) = M \\ & = (1, 27) & (M) \end{aligned}$$

$$\begin{aligned} e_2 = 1 : \quad & (x_t, y_t) = 2M + M \\ & = (33, 490) + (1, 27) = (559, 362) & (3M) \end{aligned}$$

$$\begin{aligned} e_1 = 0 : \quad & (x_t, y_t) = 2(2M + M) \\ & = (559, 362) + (559, 362) = (540, 630) & (6M) \end{aligned}$$

$$\begin{aligned} e_0 = 1 : \quad & (x_t, y_t) = 2(2(2M + M)) + M \\ & = (209, 207) + (1, 27) = (13, 527) & (13M) \end{aligned}$$

Alice sends $C = (13, 527)$ to Bob.

Bob computes $M = dC = 37C$ on E_{667} to obtain M.

$$d = 37 = 100101_2 = d_5d_4d_3d_2d_1d_0$$

$$\begin{aligned} d_5 = 1 : \quad & (x_t, y_t) = C = (13, 527) & (C) \\ d_4 = 0 : \quad & (x_t, y_t) = 2C = (56, 306) & (2C) \\ d_3 = 0 : \quad & (x_t, y_t) = 2(2C) = (281, 41) & (4C) \\ d_2 = 1 : \quad & (x_t, y_t) = 2(4C) + C = (559, 305) & (9C) \\ d_1 = 0 : \quad & (x_t, y_t) = 2(9C) = (540, 37) & (18C) \\ d_2 = 1 : \quad & (x_t, y_t) = 2(18C) + C = (1, 27) & (37C) \end{aligned}$$

4 Cryptanalysis of KMOV cryptosystem with short secret exponent

The security of the KMOV cryptosystem is based on the difficulty of finding the secret key d. If an attacker factors n as pq, then he knows $\operatorname{lcm}(p+1, q+1)$ and he can find d from the relation $ed \equiv 1 \pmod{\operatorname{lcm}(p+1, q+1)}$. Solving a secret key d from public keys e and n is computationally equivalent to factoring a composite number n.

In this article, we are only interested in attacks using continued fractions. If $[a_0; a_1, a_2, \ldots]$ is the continued fractions of a real number α, then the convergents $\frac{p_m}{q_m}$ satisfy $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0a_1 + 1$, $q_1 = a_1$ and for $i > 1$

$$\begin{aligned} p_i &= a_ip_{i-1} + p_{i-2} \\ q_i &= a_iq_{i-1} + q_{i-2}. \end{aligned}$$

In 1990, Wiener [13] proposed a polynomial time algorithm for breaking a RSA cryptosystem, where p and q are same size and $e < n$, if the secret exponent d has at most one-quarter as many bits as the modulus 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 expansion of e/n, and therefore d can be computed from the public keys n and e. In 1997, Verheul and van Tilborg [11] proposed extension of the Wiener attack when d is few bits longer than $n^{0.25}$. The candidates for the secret exponent d are of the form $d = rq_{m+1} + sq_m$, for some positive integers r and s. In 2004. Dujella [2] described new variant of the Wiener attack. This attack is very similar to the Verheul and van Tilborg attack, but instead of exhaustive search after finding the appropriate convergent, this variant also uses estimates which follow from Diophantine approximations [2, Theorem 1].

Theorem 1 (Dujella, Worley) *Let α be an 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 some nonnegative integers m, r and s such that $rs < 2c$.

In 1995, Pinch [9] extended the Wiener attack to KMOV cryptosystem, and here we extend the Dujella variant of the Wiener attack to KMOV cryptosystem.

From $ed \equiv 1 \pmod{\operatorname{lcm}(p+1, q+1)}$ there must exist 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 that

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

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

$$\begin{aligned} ed &= \frac{k}{g} \cdot (p+1)(q+1) + 1 \\ edg &= k(p+1)(q+1) + g. \end{aligned} \qquad (4)$$

Let $d = D\sqrt[4]{n}$. Assume that $p < q < 2p$. Then $2\sqrt{n} < p + q < 2.1214\sqrt{n}$ and this implies

$$\begin{aligned} \frac{e}{n} - \frac{k}{dg} &= \frac{kn + kp + kq + k + g - kn}{ndg} \\ &= \frac{k(p+q) + k + g}{ndg} \\ &< \frac{k \cdot (2.1214\sqrt{n} + 2)}{ndg}. \end{aligned}$$

We may assume that $n > 10^8$, and we have

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

In the opposite direction we have

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

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

$$\frac{e}{n} - \frac{k}{dg} > \frac{e}{n} \cdot \frac{2\sqrt{n} + 1}{(\sqrt{n} + 1)^2} > \frac{1.9997e}{n\sqrt{n}}.$$

Let m be the largest (even) integer such that

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

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 first case we may assume that $\frac{p_{m+2}}{q_{m+2}} > \frac{k}{dg}$. We have

$$\frac{e}{n} - \frac{k}{dg} < \frac{2.1216e}{n\sqrt{n}} < \frac{2.1216}{G\sqrt{n}} = \frac{\frac{2.1216D^2g^2}{G}}{(dg)^2},$$

and from Theorem 1 we conclude that

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

where $m \geq -1$ and r, s and t are nonnegative integers satisfying $rs < 4.2432\frac{D^2g^2}{G}$ and $st < 4.2432\frac{D^2g^2}{G}$.

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

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

The determinant of the system is 1 and therefore the system has positive integer solutions:

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

If r and s small, then they can be found by an exhaustive search. Let us find upper bounds for r and s. From [5, Theorem 9 and 13] $\left(\frac{1}{q_m(q_{m+1}+q_m)} < \left|\alpha - \frac{p_m}{q_m}\right| < \frac{1}{q_m q_{m+1}}\right)$, we have $r = dgq_m\left(\frac{k}{dg} - \frac{p_m}{q_m}\right) < \frac{dg}{q_{m+1}}$. The estimate for s have two possibilities. Assume that $\frac{p_{m+1}}{q_{m+1}} - \frac{e}{n} > \frac{2.1216e}{n\sqrt{n}}$. Then

$$s = dqq_{m+1}\left(\frac{p_{m+1}}{q_{m+1}} - \frac{k}{dg}\right) < \frac{2dg}{q_{m+2}}.$$

Since

$$\frac{1}{q_{m+2}^2\left(a_{m+3}+2\right)} < \frac{e}{n} - \frac{p_{m+2}}{q_{m+2}} < \frac{2.1216e}{n\sqrt{n}} < \frac{2.1216}{G\sqrt{n}},$$

we have

$$q_{m+2} > \frac{\sqrt{G}\sqrt[4]{n}}{\sqrt{2.1216\left(a_{m+3}+2\right)}}\,.$$

Putting all these estimates together we obtain

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

Assume now that $\frac{p_{m+1}}{q_{m+1}} - \frac{e}{n} \le \frac{2.1216e}{n\sqrt{n}}$. Then

$$s = dqq_{m+1}\left(\frac{p_{m+1}}{q_{m+1}} - \frac{k}{dg}\right) < \frac{dg}{q_m},$$

and analogous to the previous case we have

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

We have $rs < 4.2432\,\frac{D^2g^2}{G}$ and (see [2]) $r = a_{m+2}s - t < a_{m+2}s$ which imply $r < \sqrt{4.2432a_{m+2}}\ \frac{Dg}{\sqrt{G}}$. We have that $s \le s_1$ where $s_1 = \left\lfloor 2\cdot\sqrt{2.1216\left(a_{m+3}+2\right)}\ \frac{Dg}{\sqrt{G}}\right\rfloor$ if $\frac{p_{m+1}}{q_{m+1}} - \frac{e}{n} > \frac{2.1216e}{n\sqrt{n}}$ and $s_1 = \left\lfloor\sqrt{2.1216\left(a_{m+2}+2\right)}\left(a_{m+1}+1\right)\ \frac{Dg}{\sqrt{G}}\right\rfloor$ if $\frac{p_{m+1}}{q_{m+1}} - \frac{e}{n} \le \frac{2.1216e}{n\sqrt{n}}$.

Let $s_0 = \left\lfloor\sqrt{4.2432}\ \frac{Dg}{\sqrt{G}\sqrt{a_{m+2}}}\right\rfloor$. We have the following upper bound for the number of possible pairs (r,s):

$$\begin{aligned} &a_{m+2}\textstyle\sum_{i=1}^{s_0-1} i + 4.2432\,\frac{D^2g^2}{G}\sum_{i=s_0}^{s_1}\frac{1}{i} < \\ &< a_{m+2}\cdot\tfrac{s_0(s_0-1)}{2} + 4.2432\,\tfrac{D^2g^2}{G}\left(1 + \textstyle\int_{s_0}^{s_1}\frac{dx}{x}\right) < \\ &< a_{m+2}\cdot\tfrac{s_0^2}{2} + 4.2432\,\tfrac{D^2g^2}{G}\left(1 + \ln\tfrac{s_1}{s_0}\right) < \\ &< 4.2432\,\tfrac{D^2g^2}{G}\left(1.5 + \ln\tfrac{s_1}{s_0}\right) < \\ &< 4.2432\,\tfrac{D^2g^2}{G}\ \left(1.1536 + \ln\left(\max\left(A,B\right)\right)\right). \end{aligned}$$

where

$$\begin{aligned} A &= 2\sqrt{a_{m+2}\left(a_{m+3}+2\right)} \\ B &= \left(a_{m+2}+1\right)\left(a_{m+1}+1\right). \end{aligned}$$

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

In the second case we assume that $\frac{p_{m+2}}{q_{m+2}} \le \frac{k}{dg}$. We search for $\frac{k}{dg}$ among the fractions of the form $\frac{k}{dg} = \frac{r'p_{m+3}+s'p_{m+2}}{r'q_{m+3}+s'q_{m+2}}$. Similar with first case we have

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

Now we have

$$\begin{aligned} r' &= dgq_{m+2}\left(\frac{k}{dg}-\frac{p_{m+2}}{q_{m+2}}\right) \\ &= dgq_{m+2}\left[\left(\frac{e}{n}-\frac{p_{m+2}}{q_{m+2}}\right)-\left(\frac{e}{n}-\frac{k}{dg}\right)\right] \\ &< dgq_{m+2}\cdot\frac{0.1219e}{n\sqrt{n}} < 0.06096\cdot\frac{dg}{q_{m+3}} \\ &< \frac{0.06096\sqrt{2.1216\left(a_{m+3}+2\right)}}{a_{m+3}\sqrt{G}}\,Dg \\ s' &= dgq_{m+3}\left(\frac{p_{m+3}}{q_{m+3}}-\frac{k}{dg}\right) \le \frac{dg}{q_{m+2}} \\ &< \frac{\sqrt{2.1216\left(a_{m+3}+2\right)}}{\sqrt{G}}\,Dg\,. \end{aligned}$$

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

$$r's' < 0.387999\,\frac{D^2g^2}{G}.$$

We will now consider how one could test whether a guess of k and dg is correct. Since $g < k$ we have from (4) that guess of $(p+1)(q+1)$ is $\left\lfloor\frac{e\cdot dg}{k}\right\rfloor$ and 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

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

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:

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

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 was the remainder when edg was divided by k. We can also recover p and q easily from $\frac{p+q}{2}$ and $\frac{q-p}{2}$.

Example 3 Let

$$n = 160330625582478987749371174133657907449 17$$

and

$$e = 89570196445597558758430555068684159360 7.$$

The first 19 partial quotiens of the continued expansion of $\frac{e}{n}$ are

$$[0,17,1,8,1,3436,1,4,2,5,1,4,1,5,5,1,1,3,2,\ldots]\,,$$

and the some convergents are

$$\frac{p_0}{q_0}=0,\quad \frac{p_1}{q_1}=\frac{1}{17},\quad \frac{p_2}{q_2}=\frac{1}{18},\quad \frac{p_3}{q_3}=\frac{9}{61},\ \ldots,$$

$$\frac{p_{14}}{q_{14}}=\frac{83158371}{1488534599},\qquad \frac{p_{15}}{q_{15}}=\frac{430058380}{7698043751},$$

$$\frac{p_{16}}{q_{16}}=\frac{513216751}{9186578350},\qquad \frac{p_{17}}{q_{17}}=\frac{943275131}{16884622101},\ldots$$

We find that

$$\frac{83158371}{1488534599} < \frac{e}{n} - \frac{2.1216e}{n\sqrt{n}} < \frac{513216751}{9186578350}\,,$$

and have $m = 14$. We are searching for the secret number dg between the numbers of the form $7698043751r + 1488534599s$ or $9186578350s - 7698043751t$ or $16884622101r' + 9186578350s'$. By applying the above mentioned test, we find that $s = 494414887$ and $t = 261$ gives the correct value for secret key d (i.e. for k and dg). We have secret key $d = 2782668710135556079$ and the factorization of $n = pq$ is achieved, where the factors are $p = 126621133370427318341$ and $q = 126622327027697104337$.

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 $s = 494414887$, but the other number $r = 494414626$ is much bigger than the number $t = 261$.

Example 4 We take now the 41 digit example.

$$n = 16033062558247898774937117413365790744917.$$

Among 1000000 trials with randomly chosen private key d such that $\frac{1}{3}n^{0.25} < d < 10^9 \cdot n^{0.25}$, we have following results. In 988974 (98.90%) trials we have that $\frac{p_{m+2}}{q_{m+2}} > \frac{k}{dg}$. The maximal value of $\min\{rs, st\}$ is 2410094076733959020 and it is attained for $d = 3730709572904400293$. The average value of $\min\{rs, st\}$ is 81126922686797477.50. The maximal value of $\min\{\frac{Grs}{D^2g^2}, \frac{Gst}{D^2g^2}\}$ is 3.9541 and it is attained for $d = 1771893280839858823$. The average value of these minimums for d in the given interval is 0.8329.

In 11026 (1.10%) trials we have that $\frac{p_{m+2}}{q_{m+2}} \leq \frac{k}{dg}$. The maximal value of products $r's'$ is 3898654431581218l0 and it is attained for $d = 2056384316432564443$. The average value of these products $r's'$ is 2879889251373413.87. The maximal value of $\frac{Gr's'}{D^2g^2}$ is 0.1133 and it is attained for $d = 7551555910757195559$. The average value of these products is 0.0297.

Note that KMOV cryptosystem with 1024–bit modulus n is factoring–secure. In this case, Pinch [9] showed that the KMOV cryptosystem is insecure for 256–bit d and the attack described in this paper shows that it is insecure for 270–bit secret key d.

References

[1] W. Diffie, E. Hellman: New directions in cryptography, IEEE Transactions on Information Theory, **22**(1976), pp. 644–654.

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

[3] A. Dujella: Number theory in cryptography, Lecture notes, available at `http://web.math.hr/~duje/tbkript/tbkriptlink.pdf`, Accessed: 9^{th} May 2008.

[4] A. Dujella, B. Ibrahimpašić: On Worley's theorem in Diophantine approximations, 13 pp, preprint.

[5] A. Ya. Khinchin: Continued fractions, Dover, New York, USA, 1997.

[6] N. Koblitz: Elliptic curve cryptosystems, Mathematics of Computation **48**(1987), pp. 203–209.

[7] K. Koyama, U. M. Maurer, T. Okamoto, S. A. Vanstone: New public–key schemes based on elliptic curves over the ring $\mathbf{Z_n}$, Advances in Cryptology - Crypto '91, Lecture Notes in Computer Science, vol. 576, Springer–Verlag, 1991, pp. 252–266.

[8] V. S. Miller: Use of elliptic curves in cryptography, Advances in Cryptology - Crypto '85, Lecture Notes in Computer Science, vol. 218, Springer–Verlag, 1986, pp. 417–426.

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

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

[11] E. R. Verheul, H. C. A. van Tilborg: Cryptanalysis of 'less short' RSA secret exponents, Applicable Algebra Engineering Communication and Computing **8**(1997), pp. 425–435.

[12] L. C. Washington: Elliptic curves: Number theory and Cryptography, 2nd edition, Chapmann & Hall/CRC, Boca Raton, 2008.

[13] M. J. Wiener: Cryptanalysis of short RSA secret exponents, IEEE Trans. on Information Theory **36**(1990), pp. 553–558.

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