New Partial Key Exposure Attacks on RSA

Johannes Blömer, Alexander May

Faculty of Computer Science, Electrical Engineering and Mathematics
Paderborn University
33102 Paderborn, Germany
{*bloemer,alexx*}*@uni-paderborn.de*

Abstract. In 1998, Boneh, Durfee and Frankel [4] presented several attacks on RSA when an adversary knows a fraction of the secret key bits. The motivation for these so-called partial key exposure attacks mainly arises from the study of side-channel attacks on RSA. With side channel attacks an adversary gets either most significant or least significant bits of the secret key. The polynomial time algorithms given in [4] only work provided that the public key e is smaller than $N^{\frac{1}{2}}$. It was raised as an open question whether there are polynomial time attacks beyond this bound. We answer this open question in the present work both in the case of most and least significant bits. Our algorithms make use of Coppersmith's heuristic method for solving modular multivariate polynomial equations [8]. For known most significant bits, we provide an algorithm that works for public exponents e in the interval $[N^{\frac{1}{2}}, N^{0.725}]$. Surprisingly, we get an even stronger result for known least significant bits: An algorithm that works for all $e < N^{\frac{7}{8}}$.
We also provide partial key exposure attacks on fast RSA-variants that use Chinese Remaindering in the decryption process (e.g. [20, 21]). These fast variants are interesting for time-critical applications like smart-cards which in turn are highly vulnerable to side-channel attacks. The new attacks are provable. We show that for small public exponent RSA half of the bits of $d_p = d \bmod p - 1$ suffice to find the factorization of N in polynomial time. This amount is only a quarter of the bits of N and therefore the method belongs to the strongest known partial key exposure attacks.
Keywords: RSA, known bits, lattice reduction, Coppersmith's method

1 Introduction

Let (N, e) be an RSA public key with $N = pq$, where p and q are of equal bit-size. The secret key d satisfies $ed = 1 \bmod \phi(N)$.

In 1998, Boneh, Durfee and Frankel [4] introduced the following question: How many bits of d does an adversary need to know in order to factor the modulus N? In addition to its theoretical impact on understanding the complexity of the RSA-function, this is an important practical question arising from the intensive study of side-channel attacks on RSA in cryptography (e.g. fault attacks, timing attacks, power analysis, see for instance [6, 15, 16]).

In many scenarios, an attacker using a side-channel attack either succeeds to obtain the most significant bits (MSBs) or the least significant bits (LSBs) of d in *consecutive order*. Whether he gets MSBs or LSBs depends on the different ways of computing an exponentiation with d during the decryption process. Therefore in this work, we just focus on the case where an adversary knows either MSBs or LSBs of d and we ignore attacks where an adversary has to know both sorts of bits or intermediate bits.

Cases have been reported in the literature [9] where side-channel attacks are able to reveal a fraction of the secret key bits, but fail to reveal the entire key. For instance it is often the case that an attacker gets the next bit of d under the conditional probability that his hypothesis of the previous bits is correct. Hence, it gets harder and harder for him to make a correct guess with a certain probability. This makes it essential to know how many bits of d suffice to discover the whole secret information.

Boneh, Durfee and Frankel [4] were the first that presented polynomial time algorithms when an attacker knows only a fraction of the bits. In the case of known least significant bits, they showed that for low public exponent RSA (e.g. $e = \text{poly}(\log N)$) a quarter of the bits of d are sufficient to find the factorization of N. Their method makes use of a well-known theorem due to Coppersmith [8]: Given half of the bits of p, the factorization of N can be found in polynomial time.

Considering known MSBs, Boneh, Durfee and Frankel presented an algorithm that works for all $e < N^{\frac{1}{2}}$, again using Coppersmith's theorem. However it remained an open question in [4] whether there are polynomial time algorithms that find the factorization of N for *values of e substantially larger than $N^{\frac{1}{2}}$* given only a subset of the secret key bits.

In this work, we answer this question both in the case of known MSBs and of known LSBs.

MSBs of d known:
We present a method that works for all public exponents e in the interval $[N^{\frac{1}{2}}, N^{0.725}]$. The number of bits of d that have to be known increases with e. Let us provide some examples of the required bits: For $e = N^{0.5}$ one has to know half of the MSBs of d, for $e = N^{0.55}$ a 0.71-fraction suffices whereas for $e = N^{0.6}$ a fraction of 0.81 is needed to factor N.

In contrast to Boneh, Durfee and Frankel we do not use Coppersmith's result for known bits of p. Instead we directly apply Coppersmith's method for finding roots of modular multivariate polynomial equations [8]. This method has many applications in cryptography. Since it is a heuristic in the multivariate case, our result is heuristic as well. However, in various other applications of Coppersmith's method (see [1, 3, 10, 14]) a systematic failure of the multivariate heuristic has never been reported. Hence the heuristic is widely believed to work perfectly in practice. We also provide various experiments that confirm the reliability: None of our experiments failed to yield the factorization of N.

In Figure 1 we illustrate our result for MSBs. The size of the fraction of the bits that is needed in our attack is plotted as a function of the size of the public exponent e. We express the size of e in terms of the size of N (i.e. we use $\log_N(e)$). For a comparison with previous results, we also include in our graphs the results of Boneh, Durfee and Frankel. The marked regions in Figure 1 are the feasible regions for the various approaches.

Note that the area belonging to BDF2 requires that the factorization of e is known. The result BDF3 is not explicitly mentioned as a polynomial time algorithm in [4], but can be easily derived from a method stated by the same authors in [5]: The upper $\log_N(e)$ bits of d immediately yield half of the MSBs of d and the attacker can use the remaining quarter of bits to factor N.

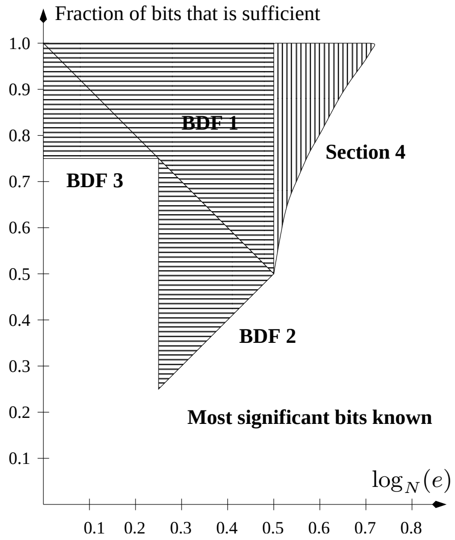

Fig. 1. The results for known MSBs of d

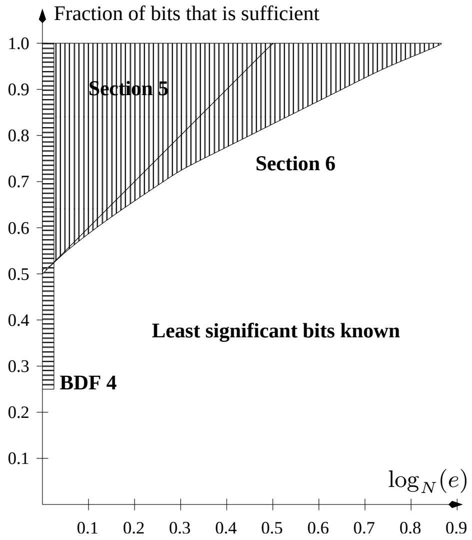

Fig. 2. The results for known LSBs of d

LSBs of d known:
We start by proving a result for all but a negligible fraction of the public exponents $e < N^{\frac{1}{2}}$. Previously, only polynomial time algorithms for e of the order $\text{poly}(\log N)$ were known [4]. Our approach uses a 3-dimensional lattice to find the factorization of N using a single lattice basis reduction, whereas the method in [4] requires about e lattice reductions. We tested our attack with the frequently used RSA-exponent $e = 2^{16} + 1$. Our algorithm is faster than the method in [4] but requires more bits of d.

Interestingly, our approach makes use of the linear independence of two sufficiently short vectors in the lattice and we do not need to apply Coppersmith's heuristic in this case. This makes our method rigorous and at the same time introduces a new method to solve modular multivariate polynomial equations of a special form. Therefore we believe that our approach is of independent interest.

Next, we generalize the 3-dimensional approach to multi-dimensional lattices. This improves the bound up to all $e < N^{\frac{7}{8}}$, which is the largest bound for e in partial key exposure attacks that is known up to now. Unfortunately, since our attack relies on Coppersmith's method for modular multivariate polynomial equations, it becomes heuristic. But again in our experiments, we could not find a single failure of the multivariate heuristic. The results are illustrated in Figure 2 in the same fashion as before.

We raise the question whether it is possible to derive results for all keys $e < \phi(N)$. In the light of our new results, this bound does not seem to be out of reach. Maybe a modification of our lattices could already suffice (e.g. using non-triangular lattice bases), but at the moment this is an open question.

Known bits in CRT-variants:
We present results on known bits of $d_p = d \bmod p - 1$ (and symmetrically on $d_q = d \bmod q - 1$). The value d_p is used in fast Chinese Remainder variants of the decryption process. This includes the well-known Quisquater-Couvreur method [21]. With suitable modifications, the attack applies also to other fast RSA-variants like for instance Takagi's scheme [20], which uses a modulus of the form $p^k q$.

These fast variants of RSA are especially interesting for time-critical applications. Therefore they are frequently used on smart-cards. On the other hand, it is well-known that smart-cards are highly vulnerable to different sorts of side-channel attacks. Hence it is of important practical interest to study the complexity of partial key exposure attacks for CRT-variants.

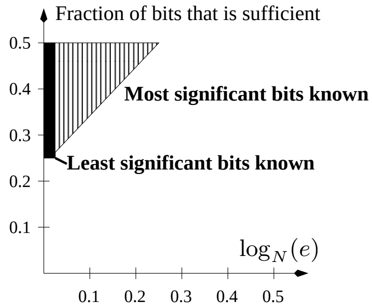

Fig. 3. LSBs/MSBs of d_p.

We provide provable attacks for both cases: LSBs and MSBs. Interestingly, in our proofs we use a less known variant of a result of Coppersmith [8] that is due to Howgrave-Graham. Coppersmith showed that an approximation of p up to an additive error of $N^{\frac{1}{4}}$ yields the factorization of N. Howgrave-Graham [13] observed that an approximation of kp for some (unknown) k with the same error bound already suffices.

We prove that for low public exponents e (i.e. $e = \text{poly}(\log N)$), half of the LSBs of d_p always suffice to factor N. Therefore the attack is a threat to RSA-implementations with the commonly used public exponent $e = 2^{16} + 1$. Note that half of the bits of d_p is only an amount of a quarter of the bits of N and therefore the result is as strong as the best known partial key exposure attacks.

In the case of known MSBs of d_p, we present an algorithm that even works for all $e < N^{\frac{1}{4}}$ in polynomial time. Again for low public exponent RSA, it requires only half of the MSBs of d_p in order to factor N. The results are illustrated in Figure 3.

Detailed overview:
We briefly overview all known polynomial time partial key exposure attack by giving the precise functions of the bits that have to be known. Let $\alpha = \log_N(e)$ denote the size of e in terms of N. In Figure 4, the upper half of the table states the results for known MSBs whereas the lower half is dedicated to the results for known LSBs. The attacks for known bits of d_p are stated in the last lines of each half.

	$\alpha = \log_N(e)$	Fraction of bits that is needed	Restriction/Comment
BDF [4]	$[\frac{1}{4}, \frac{1}{2}]$	α	e prime/known fact.
BDF [4]	$[0, \frac{1}{2}]$	$1-\alpha$	$\frac{d}{\phi(N)} = \Omega(1)$
Section 4	$[\frac{1}{2}, \frac{\sqrt{6}-1}{2}]$	$\frac{1}{8}\left(3 + 2\alpha + \sqrt{36\alpha^2 + 12\alpha - 15}\right)$	heuristic
BDF [5]	$[0, \frac{1}{2}]$	$\frac{3}{4}$	$\frac{d}{\phi(N)}, \frac{\lvert p-q\rvert}{\sqrt{N}} = \Omega(1)$
Section 2	$[0, \frac{1}{4}]$	$\frac{1}{4} + \alpha$	bits of d_p
BDF [5]	$\mathcal{O}(\log_N \log N)$	$\frac{1}{4}$	$N = 3 \bmod 4$
Section 5	$[0, \frac{1}{2}]$	$\frac{1}{2} + \alpha$	all but $O(N^{\alpha-\epsilon})$ e's
Section 6	$[0, \frac{7}{8}]$	$\frac{1}{6} + \frac{1}{3}\sqrt{1+6\alpha}$	heuristic
Section 2	$\mathcal{O}(\log_N \log N)$	$\frac{1}{4}$	bits of d_p

Fig. 4. Detailed summary of the results

The paper is organized as follows: In Section 2, we present our methods for the CRT-variants. Here we use lattice reduction methods only as a black-box. In order to give the more elaborate results for partial key exposure attacks with large public exponent, we have to define some lattice notation in Section 3. The method for MSBs is presented in Section 4, the LSB-attacks are given in Section 5 and 6.

2 Known MSBs/LSBs and Chinese Remaindering

Throughout this work we will consider RSA-public keys (N, e) with $N = pq$, where p and q are of equal bit-size. Therefore $p, q \leq 2\sqrt{N}$. Furthermore, we assume wlog that $p \leq q$ which implies $p \leq \sqrt{N}$ and

$$p + q \leq 3\sqrt{N}.$$

The secret exponent d corresponding to (N, e) satisfies the equality $ed = 1 \bmod \phi(N)$, where $\phi(N)$ is the Euler totient function.

We will often talk of known most or least significant bits (MSBs/LSBs) of d, but we want to point out that this should only be understood as a helpful simplification to explain our results in the context of side-channel attacks. To be more precise, when we talk of k known LSBs of d, then in fact we only need to know integers d_0, M such that $d_0 = d \bmod M$, where $M \geq 2^k$. Thus, $M = 2^k$ is only the special case where we really know the bits. Analogously, in the case of known MSBs: We do not really need to know the MSBs but only an approximation $\tilde{d}$ of d such that $|d - \tilde{d}|$ can be suitably upper-bounded.

In order to speed up the decryption/signing process, it is common practice to use the values $d_p = d \bmod p - 1$ and $d_q = d \bmod q - 1$. To sign m, one computes $m^{d_p} \bmod p$ and $m^{d_q} \bmod q$ and combines the results using the Chinese Remainder Theorem (CRT).

These fast RSA-variants are especially interesting for time-critical applications like smart-cards, which are highly vulnerable to side-channel attacks. However, it has never been studied how many bits of d_p (or symmetrically of d_q) suffice in order to find the factorization of N. We present two provable results for RSA-variants with CRT in this section.

Both of our proofs use the following variation of a well-known theorem of Coppersmith [8] that is due to Howgrave-Graham. Coppersmith showed how to factor N given half of the MSBs of p. Howgrave-Graham [13] observed that this holds in more general form for the MSBs of multiples of p.

Theorem 1 (Howgrave-Graham) *Let $N = pq$ be an RSA-modulus and k be an unknown integer which is not a multiple of q. Given an approximation of kp with additive error at most $N^{\frac{1}{4}}$, the factorization of N can be found in polynomial time.*

First, we consider the case of known LBSs of d_p. We show that whenever the public exponent e is of size poly$(\log N)$, then half of the lower bits of d_p are sufficient to find the factorization of N in polynomial time.

Theorem 2 *Let (N, e) be an RSA public key with $N = pq$ and secret key d. Let $d_p = d \bmod p - 1$. Given d_0, M with $d_0 = d_p \bmod M$ and*

$$M \geq N^{\frac{1}{4}}.$$

Then the factorization of N can be found in time $e \cdot poly(\log N)$.

Proof: We know that

$$ed_p - 1 = k(p - 1)$$

for some $k \in \mathbb{N}$. Since $d_p < p-1$, we know that $k = \frac{ed_p-1}{p-1} < e$. Let us write $d_p = d_1 M + d_0$, where $d_1 < \frac{d_p}{M} < \frac{p}{M} \leq N^{\frac{1}{4}}$. We can rewrite our equation as

$$ed_0 + k - 1 = kp - eMd_1.$$

Let E be the inverse of eM modulo N, e.g. there exist a $c \in \mathbb{N}$ such that $E \cdot eM = 1 + cN$ (if E does not exist, we obtain the factorization of N). Multiplying the above equation by E yields

$$E(ed_0 + k - 1) = (Ek - cqd_1)p - d_1.$$

The only unknown parameter on the left hand side of the equation is k. We make a brute force search for k in the interval $[1, e)$. The correct guess of k gives us a multiple of p up to an additive error $d_1 < N^{\frac{1}{4}}$. Thus, when the algorithm of Theorem 1 is applied to the correct guess of k, we obtain the factorization of N. Note that q divides the term $Ek - cqd_1$ iff q divides k which is easily testable (q cannot divide k in the case $e < q$). This concludes the proof of the theorem. $\square$

In our second approach, we consider the case when MSBs of d_p are known.

Theorem 3 *Let (N, e) be an RSA public key with secret key d and $e = N^{\alpha}$ for some $a \in [0, \frac{1}{4}]$. Furthermore, let $d_p = d \bmod p - 1$. Given $\tilde{d}$ with*

$$|d_p - \tilde{d}| \leq N^{\frac{1}{4} - \alpha}.$$

Then N can be factored in polynomial time.

Proof: We start again by looking at the equation $ed_p - 1 = k(p-1)$. Since $d_p < p-1$, we know that $k < N^{\alpha}$, which implies that q cannot divide k. Compute $\tilde{p} = e\tilde{d} - 1$. Now, $\tilde{p}$ is an approximation of kp up to an additive error of at most

$$|\tilde{p} - kp\,| = |e(\tilde{d} - d_p) - k| \leq N^{\frac{1}{4}} + N^{\alpha} \leq 2N^{\frac{1}{4}}.$$

Thus, either $\tilde{p} + N^{\frac{1}{4}}$ or $\tilde{p} - N^{\frac{1}{4}}$ is an approximation of kp with error at most $N^{\frac{1}{4}}$. Applying the algorithm of Theorem 1 to both values yields the factorization of N. $\square$

3 Preliminaries on Lattices

Since our partial key exposure attacks for large public exponents use polynomial arithmetic, we introduce some helpful notations. Let $f(x, y) = \sum_{i,j} a_{i,j} x^i y^j$ be a bivariate polynomial with coefficients $a_{i,j} \in \mathbb{Z}$. All terms $x^i y^j$ with non-zero coefficients are called monomials. The coefficient vector of f is defined by the vector of the coefficients $a_{i,j}$. We define the norm of f as the Euclidean norm of the coefficient vector: $\|f\|^2 = \sum_{i,j} a_{i,j}^2$. The definitions for trivariate polynomials are analogous. In the following, we state a few basic facts about lattices and lattice basis reduction and refer to the textbooks [7, 11, 18] for an introduction to the theory of lattices.

Let $v_1, \ldots, v_n \in \mathbb{R}^n$ be linearly independent vectors. A lattice L spanned by $\{v_1, \ldots, v_n\}$ is the set of all integer linear combinations of $v_1, \ldots, v_n$. We call n the dimension of L, which we denote by $\dim(L)$.

The set $B = \{v_1, \ldots, v_n\}$ is called a basis of L, the $(n \times n)$-matrix consisting of the row vectors $v_1, \ldots, v_n$ is called basis matrix. A basis of L can be transformed into another basis by applying an unimodular transformation to the basis matrix. The determinant $\det(L)$ is the absolute value of the determinant of a basis matrix.

The famous L^3-lattice reduction algorithm of Lenstra, Lenstra and Lovász [17] can be used to approximate a shortest vector.

Theorem 4 (Lenstra, Lenstra, Lovász) *Let $L \in \mathbb{Z}^n$ be a lattice spanned by $\{v_1, \ldots, v_n\}$. The L^3-algorithm outputs in polynomial time a reduced lattice basis $\{v_1', \ldots, v_n'\}$ with*

$$\|v_i'\| \leq 2^{\frac{n(n-1)+(i-1)(i-2)}{4(n-i+1)}} \det(L)^{\frac{1}{n-i+1}} \qquad \text{for } i = 1, \ldots, n.$$

This theorem can easily be proven using [7], Theorem 2.6.2.

In Sections 4 and 6, we will use a heuristic of Coppersmith [8] for multivariate modular polynomial equations. This heuristic has proven to be very useful in many attacks (see [1, 3, 10, 14]). We made various experiments for our approaches and the methods never failed to reveal the desired factorization of N. Therefore, we make the following assumption which refers to the only heuristic part in our computations of Section 4 and 6.

Assumption 5 *The resultant computations for the multivariate polynomials constructed in our approaches yield non-zero polynomials.*

4 MSBs known: A method for $e \in [N^{\frac{1}{2}}, N^{0.725}]$

In this section, we present an attack on RSA for public exponents e in the interval $[N^{\frac{1}{2}}, N^{\frac{\sqrt{6}-1}{2}}]$ given most significant bits of d. This answers an open question of Boneh, Durfee and Frankel [4] whether there are partial key exposure attacks in the case of known MSBs beyond the bound $e = \sqrt{N}$. Our approach makes use of Coppersmith's method for modular polynomial equations in the trivariate case.

Theorem 6 *Under Assumption 5, for every $\epsilon > 0$ there exists an integer N_0 such that for every $N > N_0$ the following holds:*
Let (N, e) be an RSA public key, where $\alpha = \log_N(e)$ is in the range $[\frac{1}{2}, \frac{\sqrt{6}-1}{2}]$. Given an approximation $\tilde{d}$ of d with

$$|d - \tilde{d}| \leq N^{\frac{1}{8}\left(5-2\alpha-\sqrt{36\alpha^2+12\alpha-15}\right)-\epsilon}.$$

Then N can be factored in time polynomial in $\log N$.

Before we start to prove Theorem 6, in Figure 5 we provide some experimental results to give an idea of the amount of bits that is needed in our partial key exposure attack. The experiments also confirm the reliability of the multivariate heuristic and support our Assumption 5.

Define $\delta = \frac{1}{8}\left(5 - 2\alpha - \sqrt{36\alpha^2 + 12\alpha - 15}\right) - \epsilon$. Then a fraction of $1-\delta$ of the MSBs of d is required (asymptotically) for the new attack. For $\alpha = 0.55$ this is a 0.710-fraction and for $\alpha = 0.6$ we require a 0.809-fraction. Note that these theoretical bounds hold as N and the lattice dimension go to infinity. All of our experiments were carried out on a 500-MHz workstation using Shoup's NTL [19].

N	e	**known MSBs**	Lattice parameters	L^3-time
1000 bit	*600 bit*	**955 bit**	$m = t = 1,\ \dim(L) = 7$	1 sec
1000 bit	550 bit	**855 bit**	$m = t = 1,\ \dim(L) = 7$	1 sec
1000 bit	*600 bit*	**905 bit**	$m = t = 2,\ \dim(L) = 19$	40 sec
1000 bit	550 bit	**810 bit**	$m = t = 2,\ \dim(L) = 19$	40 sec
1000 bit	*600 bit*	**880 bit**	$m = t = 3,\ \dim(L) = 50$	57 min
1000 bit	550 bit	**785 bit**	$m = t = 3,\ \dim(L) = 50$	72 min

Fig. 5. Experimental results for known MSBs

Proof (Theorem 6). : We start by looking at the public key equation

$$ed - 1 = k\phi(N), \qquad \text{where } k \in \mathbb{Z}. \tag{1}$$

Boneh, Durfee and Frankel [4] observed that a suitable fraction of the MSBs of d yields the parameter k. The main drawback of the methods presented in [4] is that they all require that k is known exactly. This restricts the methods' usability to public exponents $e \leq \sqrt{N}$.

Now let us relax this restriction and look at the case where one obtains only an approximation $\tilde{k}$ of k. Let $\tilde{k} = \frac{e\tilde{d}-1}{N+1}$, then

$$
\begin{aligned}
|k-\tilde{k}| &= \left|\frac{ed-1}{\phi(N)} - \frac{e\tilde{d}-1}{N+1}\right| \\
&= \left|\frac{(ed-1)(N+1)-(e\tilde{d}-1)(N+1-(p+q))}{\phi(N)(N+1)}\right| \\
&\leq \left|\frac{e(d-\tilde{d})}{\phi(N)}\right| + \left|\frac{(p+q)(e\tilde{d}-1)}{\phi(N)(N+1)}\right| \leq \frac{e}{\phi(N)}(N^{\delta}+3N^{-\frac{1}{2}}\tilde{d})
\end{aligned}
$$

We claim that the hard case is the one where the term $N^{-\frac{1}{2}}\tilde{d}$ dominates N^{δ}. Let us first assume the opposite, i.e. $N^{\delta} > N^{-\frac{1}{2}}\tilde{d}$. In this case, $|k-\tilde{k}|$ can be bounded by $N^{\alpha+\delta-1}$, where we neglect low order terms. Hence whenever $\alpha+\delta-1 \leq 0$, then k can be determined exactly. Note that the condition in Theorem 6 implies the desired inequality $\delta \leq 1-\alpha$.

But if k is known, we can compute $p+q = N+1-k^{-1} \bmod e$. On the other hand $e \geq N^{\frac{1}{2}}$ and therefore we get $p+q$ over the integers and not modulo e. This leads to the factorization of N.

Hence, we assume in the following that $N^{-\frac{1}{2}}\tilde{d} \geq N^{\delta}$. In this case, we can bound $|k-\tilde{k}|$ by $4N^{\alpha-\frac{1}{2}}$.

Now, let us define $d_0 = d-\tilde{d}$ and $k_0 = k-\tilde{k}$. Then, we can reformulate equation (1) as

$$e(\tilde{d}+d_0)-1 = (\tilde{k}+k_0)\phi(N).$$

This can also be written as

$$ed_0 + (\tilde{k}+k_0)(p+q-1) + e\tilde{d}-1 = (\tilde{k}+k_0)N. \tag{2}$$

Equation (2) gives us a trivariate polynomial

$$f_N(x,y,z) = ex + (\tilde{k}+y)z + e\tilde{d}-1$$

with the root $(x_0,y_0,z_0) = (d_0,k_0,p+q-1)$ modulo N. Define the upper bounds $X = N^{\delta}$, $Y = 4N^{\alpha-\frac{1}{2}}$ and $Z = 3N^{\frac{1}{2}}$. Then, we have $x_0 \leq X$, $y_0 \leq Y$ and $z_0 \leq Z$.

Now we use Coppersmith's method [8] in order to construct from $f_N(x,y,z)$ a polynomial $f(x,y,z)$ with the same root (x_0,y_0,z_0) over $\mathbb{Z}$ (and not just modulo N). The following theorem due to Howgrave-Graham [12] is a convenient reformulation of Coppersmith's method.

Theorem 7 (Howgrave-Graham) *Let $f(x,y,z)$ be a polynomial that is a sum of at most ω monomials. Suppose that*

(1) $f(x_0,y_0,z_0) = 0 \bmod N^m$, where $|x_0| \leq X$, $|y_0| \leq Y$ and $|z_0| \leq Z$
(2) $\|f(xX,yY,zZ)\| < \frac{N^m}{\sqrt{\omega}}$.

Then $f(x_0,y_0,z_0) = 0$ holds over the integers.

Next, we construct polynomials that all satisfy condition *(1)* of Howgrave-Graham's Theorem. Thus, every integer linear combination of these polynomials also satisfies the first condition. We search among these linear combinations for a polynomial f that satisfies condition *(2)*. This will be done using the L^3-lattice reduction algorithm.

Let us start by defining the following polynomials $g_{i,j}(x, y, z)$ and $h_{i,j}(x, y, z)$ for some fixed integers m and t:

$$\begin{aligned} g_{i,j,k} &= x^{j-k} z^k N^i f_N^{m-i} && \text{for } i = 0, \dots, m;\ j = 0, \dots, i;\ k = 0, \dots, j \\ h_{i,j,k} &= x^j y^k N^i f_N^{m-i} && \text{for } i = 0, \dots, m;\ j = 0, \dots, i;\ k = 1, \dots, t \end{aligned}$$

The parameter t has to be optimized as a function of m.

One can build a lattice $L(m)$ by using the coefficient vectors of the polynomials $g_{i,j,k}(xX, yY, zZ)$ and $h_{i,j,k}(xX, yY, zZ)$ as basis vectors for a basis $B(m)$ of $L(m)$. The following lemma shows, that the L^3-algorithm always finds at least three different vectors in $L(m)$ that satisfy condition *(2)* of Howgrave-Graham's Theorem. The proof makes use of Theorem 4.

Lemma 8 *Let $X = N^\delta$, $Y = N^{\alpha - \frac{1}{2}}$ and $Z = N^{\frac{1}{2}}$. Then one can find three linearly independent vectors in $L(m)$ with norm smaller than $\frac{N^m}{\sqrt{\dim L(m)}}$ using the L^3-algorithm.*

Proof: Let $n = \dim L(M)$ denote the lattice dimension. We want to find a reduced basis of $L(m)$ with three basis vectors smaller than $\frac{N^m}{\sqrt{n}}$. Applying Theorem 4, we know that for an L^3-reduced basis $\{v_1', v_2', \dots, v_n'\}$

$$\|v_1'\| \le \|v_2'\| \le \|v_3'\| \le 2^{\frac{n(n-1)+2}{4(n-2)}} \det L(M)^{\frac{1}{n-2}}.$$

Since we need $\|v_3'\| < \frac{N^m}{\sqrt{n}}$, we have to satisfy the condition

$$\det(L) < cN^{m(n-2)},$$

where $c = 2^{-\frac{n(n-1)+2}{4}} n^{-\frac{n-2}{2}}$ does not depend on N and therefore contributes to the error term ϵ.

Most of the following computations are straightforward but tedious. So we only sketch the rest of the proof. Let $t = \tau m$, then the determinant of $L(M)$ is

$$\det L(M) = \left(N^{8\tau+3} X^{4\tau+1} Y^{6\tau^2+4\tau+1} Z^{4\tau+2} \right)^{\frac{1}{24} m^4 (1+o(1))}.$$

Using the bounds $X = N^\delta$, $Y = 4N^{\alpha - \frac{1}{2}}$ and $Z = 3N^{\frac{1}{2}}$ we obtain

$$\det L(M) = N^{\frac{1}{24} m^4 (3\tau^2(2\alpha-1) + 4\tau(\delta+\alpha+2) + \delta + \alpha + \frac{7}{2})(1+o(1))}.$$

An easy calculation shows that $n = \frac{1}{24} m^3 (12\tau + 4)(1 + o(1))$. Neglecting low order terms, our condition simplifies to

$$3\tau^2(2\alpha - 1) + 4\tau(\delta + \alpha - 1) + \delta + \alpha - \frac{1}{2} < 0.$$

The left hand side is minimized for the choice $\tau = \frac{2}{3}\frac{1-\delta-\alpha}{2\alpha-1}$. Plugging this value in, we obtain the desired condition

$$\delta \leq \frac{1}{8}\left(5 - 2\alpha - \sqrt{36\alpha^2 + 12\alpha - 15}\right),$$

which concludes the proof. ◻

Combining Theorem 7 and Lemma 8, from the three vectors with norm smaller than $\frac{N^m}{\sqrt{\dim L(m)}}$ we obtain three polynomials $f_1(x, y, z)$, $f_2(x, y, z)$ and $f_3(x, y, z)$ with the common root (x_0, y_0, z_0). Our goal is to extract the value $z_0 = p+q-1$. The equation $N = pq$ together with the number z_0 yields the factorization of N. Therefore, we take the resultants $\mathrm{res}_x(f_1, f_2)$ and $\mathrm{res}_x(f_1, f_3)$ with respect to x. The resulting polynomials g_1 and g_2 are bivariate polynomials in y and z. In order to remove the unknown y, we compute the resultant $\mathrm{res}_y(g_1, g_2)$ which is an univariate polynomial in z. The root z_0 most be among the roots of this polynomial. Thus, if $\mathrm{res}_y(g_1, g_2)$ is not the zero polynomial (Assumption 5) then z_0 can be found by standard root finding algorithms. This concludes the proof of Theorem 6.

5 LSBs known: A provable method for $e < N^{\frac{1}{2}}$

In this section, we present a provable attack on RSA with public key $e < N^{\frac{1}{2}}$, where we know $d_0 = d \bmod M$ for some modulus M. For instance assume that an attacker succeeds to get the lower k bits of d, then $M = 2^k$.

In the following we show that whenever M is sufficiently large then N can be factored in polynomial time for all but a negligible fraction of choices for e.

Theorem 9 *Let N be an RSA-modulus and let $0 < \alpha, \epsilon < \frac{1}{2}$. For all but a $\mathcal{O}(\frac{1}{N^\epsilon})$-fraction of the public exponents e in the interval $[3, N^\alpha]$ the following holds: Let d be the secret key. Given d_0, M satisfying $d = d_0 \bmod M$ with*

$$N^{\alpha+\frac{1}{2}+\epsilon} \leq M \leq 2N^{\alpha+\frac{1}{2}+\epsilon}.$$

Then the factorization of N can be found in polynomial time.

Before we prove the theorem, we want to give some experimental results. We tested our algorithm with the commonly used public exponent $e = 2^{16} + 1$ and varying 1000-bit moduli N, where we knew 525 LSBs of d. Note that in comparison to the Boneh-Durfee-Frankel-approach for LSBs, we need about twice as many bits but in their method one has to run a lattice reduction about e times. The running time of our algorithm is about 1 second on a 500 MHz workstation. In 100 experiments, the algorithm never failed to yield the factorization of N.

Proof (Theorem 9). We start by looking at the RSA key equation $ed-1 = k\phi(N)$. Let us write $d = d_1 M + d_0$, where d_1 is the unknown part of d. Then

$$ed_1 M + k(p + q - 1) - 1 + ed_0 = kN. \tag{3}$$

Equation (3) in turn gives us a bivariate polynomial

$$f_N(x, y) = eMx + y + ed_0$$

with a root $(x_0, y_0) = (d_1, k(p + q - 1) - 1)$ modulo N. In order to bound y_0 notice that

$$k = \frac{ed - 1}{\phi(N)} < e\frac{d}{\phi(N)} < e \leq N^{\alpha}.$$

Since $d_1 \leq \frac{N}{M}$, we can set the bounds $X = N^{\frac{1}{2}-\alpha-\epsilon}$ and $Y = 3N^{\frac{1}{2}+\alpha}$ satisfying $x_0 \leq X$ and $y_0 \leq Y$.

As in Section 4, we want to transform our polynomial $f_N(x, y)$ into a polynomial $f(x, y)$ with the root (x_0, y_0) over the integers. Therefore, we apply Howgrave-Graham's Theorem (Theorem 7) in the bivariate case. For this purpose we take the auxiliary polynomials N and Nx which are both the zero polynomial modulo N. Thus, every integer linear combination $f = a_0N + a_1Nx + a_2f_N(x, y)$ has the root (x_0, y_0) modulo N.

According to the second condition of Howgrave-Graham's Theorem we have to look for an integer linear combination f satisfying $\|f(xX, yY)\| \leq \frac{N}{\sqrt{3}}$. Thus, we search for a suitably small vector in the lattice L given by the span of the row vectors of the following (3×3)-lattice base

$$B = \begin{bmatrix} N & & \\ & NX & \\ ed_0 & eMX & Y \end{bmatrix}.$$

Now, our goal is to find two linearly independent vectors $(a_0, a_1, a_2)B$ and $(b_0, b_1, b_2)B$ both having norm smaller than $\frac{N}{\sqrt{3}}$. Since L has dimension 3, we can compute two shortest linearly independent vectors in L in polynomial time using an algorithm of Blömer [2]. In practice, the L^3-algorithm will suffice.

Assume we can find two linearly independent vectors with norm smaller than $\frac{N}{\sqrt{3}}$. Then we obtain from Theorem 7 the following two equations

$$a_0N + a_1Nx_0 + a_2f_N(x_0, y_0) = 0 \text{ and}$$
$$b_0N + b_1Nx_0 + b_2f_N(x_0, y_0) = 0.$$

From equation (3) we know that $f(x_0, y_0) = kN$. Hence, our equations simplify to the linear system

$$\begin{aligned} a_1x_0 + a_2k &= -a_0 \\ b_1x_0 + b_2k &= -b_0 \end{aligned} \tag{4}$$

If $(a_0, a_1, a_2), (b_0, b_1, b_2) \in \mathbb{Z}^3$ are linearly independent and satisfy (4), then the 2-dimensional vectors $(a_1, a_2), (b_1, b_2)$ are also linearly independent. But this implies that we can determine x_0, k as the unique solution of the linear system. Afterwards, we can derive y_0 by $y_0 = kN - eMx_0 - ed_0$. Therefore, $\frac{y_0+1}{k} = p+q-1$ gives us the necessary term to factor the modulus N.

It remains to show that L contains indeed two linearly independent vectors with norm smaller than $\frac{N}{\sqrt{3}}$. The following lemma proves that this is satisfied for most choices of e using a counting argument.

Lemma 10 *Given N, α, ϵ and M as defined in Theorem 9. Then for all but $\mathcal{O}(N^{\alpha-\epsilon})$ choices of e in the interval $[3, N^\alpha]$ the following holds: Let $X = N^{\frac{1}{2}-\alpha-\epsilon}$ and $Y = 3N^{\frac{1}{2}+\alpha}$. Then the lattice L contains two linearly independent vectors with norm less than $\frac{N}{\sqrt{3}}$.*

Proof: In terms of lattice theory, we have to show that for most of the choices of e the second successive minima λ_2 of L is strictly less than $\frac{N}{\sqrt{3}}$. By Minkowski's second theorem we know that for any 3-dimensional lattice L and its successive minima $\lambda_1, \lambda_2, \lambda_3$

$$\lambda_1\lambda_2\lambda_3 \leq 2\det(L).$$

In our case $\det(L) = N^2XY$. Hence for all e such that $\lambda_1 > 6XY$, we get $\lambda_2 < \frac{N}{\sqrt{3}}$ and we are done.

Now assume $\lambda_1 \leq 6XY$. Hence, we can find coefficients $c_0, c_1, c_2 \in \mathbb{Z}$ such that $\|(c_0, c_1, c_2)B\| < 6XY$. This implies

$$|c_2| \leq 6X$$

$$\left|\frac{c_1}{c_2} + \frac{eM}{N}\right| \leq \frac{6Y}{c_2N}$$

Using $XY \leq 3N^{1-\epsilon}$, the second inequality implies

$$\left|\frac{c_1}{c_2} + \frac{eM}{N}\right| \leq \frac{18}{c_2XN^\epsilon} \tag{5}$$

Next we bound the number of e's in $[3, N^\alpha]$ that can satisfy (5) for some ratio $\frac{c_1}{c_2}$.

Since $\frac{eM}{N}$ is positive, without loss of generality we can assume that $c_1 < 0$ and $c_2 > 0$. Now we make the following series of observations.

- The difference between any two numbers of the form $\frac{eM}{N}$ is at least $\frac{M}{N} \geq N^{\alpha-\frac{1}{2}+\epsilon}$.
- If (5) is true for some ratio $\frac{c_1}{c_2}$ and some e then $\frac{eM}{N}$ must lie in the interval $\left[\frac{c_1}{c_2} - \frac{18}{c_2XN^\epsilon}, \frac{c_1}{c_2} + \frac{18}{c_2XN^\epsilon}\right]$.
- Combining the first two observations we conclude that for a fixed ratio $\frac{c_1}{c_2}$ there are at most $\frac{36}{c_2XN^{\alpha-\frac{1}{2}+2\epsilon}}$ public keys e such that (5) is satisfied.
- Since $e \leq N^\alpha$ and $M \leq 2N^{\alpha+\frac{1}{2}+\epsilon}$, we get $\frac{eM}{N} \leq 2N^{2\alpha-\frac{1}{2}+\epsilon}$. Consider a fixed but arbitrary c_2. Then (5) is satisfied for some c_1 and some public key e only if $c_1 \in [-2N^{2\alpha-\frac{1}{2}+\epsilon}c_2, -1]$.
- The previous two observations imply that for fixed c_2 the number of e's satisfying (5) is bounded by $\frac{72N^{\alpha-\epsilon}}{X}$.

– The previous observation and $c_2 \le 6X$ imply, that the number of public keys e for which (5) is satisfied for some ratio $\frac{c_1}{c_2}$ is bounded by $432N^{\alpha-\epsilon}$.

The last observation concludes the proof of Lemma 10. $\square$

6 LSBs known: A method for all e with $e < N^{\frac{7}{8}}$

In this section, we improve the approach of Section 5 by taking multi-dimensional lattices. In contrast to Section 5 our results are not rigorous. As in Section 4 they rely on Coppersmith's heuristic for multivariate modular equations. However, the results are even stronger: We obtain an attack for all $e < N^{\frac{7}{8}}$.

Theorem 11 *Under Assumption 5, for every $\epsilon > 0$ there exists N_0 such that for every $N \ge N_0$ the following holds:*
Let (N, e) be an RSA public key with $\alpha = \log_N(e) \le \frac{7}{8}$. Let d be the secret key. Given d_0, M satisfying $d = d_0 \bmod M$ with

$$M \ge N^{\frac{1}{6}+\frac{1}{3}\sqrt{1+6\alpha}+\epsilon}.$$

Then N can be factored in polynomial time.

Before we start with the proof of Theorem 11, in Figure 6 we provide some experimental results to give an idea of the number of bits that are needed in our partial key exposure attack. We fixed a bit-size of 1000 for the modulus N and used varying sizes of 300, 400 and 500 bits for e. Theorem 11 states that we need to know at least 725, 782 and 834 LSBs of d, respectively.

N	e	**known LSBs**	Lattice parameters	L^3-time
1000 bit	300 bit	**805 bit**	$m = 1, t = 0,\ \dim(L) = 3$	1 sec
1000 bit	300 bit	**765 bit**	$m = 7, t = 1,\ \dim(L) = 44$	405 min
1000 bit	400 bit	**880 bit**	$m = 3, t = 1,\ \dim(L) = 14$	40 sec
1000 bit	400 bit	**840 bit**	$m = 6, t = 1,\ \dim(L) = 35$	196 min
1000 bit	500 bit	**920 bit**	$m = 4, t = 1,\ \dim(L) = 20$	7 min
1000 bit	500 bit	**890 bit**	$m = 8, t = 2,\ \dim(L) = 63$	50 hours

Fig. 6. Experimental results for known LSBs

Proof (Theorem 11). We start by looking at the equation $ed - 1 = k\phi(N)$. As in Section 5, we write $d = d_1 M + d_0$. This gives us the equation

$$k(N - (p + q - 1)) - ed_0 + 1 = eMd_1. \tag{6}$$

From (6) we obtain the bivariate polynomial

$$f_{eM}(y, z) = y(N - z) - ed_0 + 1$$

with the root $(y_0, z_0) = (k, p + q - 1)$ modulo eM. Analogous to Section 5 we can derive the bounds $Y = N^\alpha$ and $Z = 3N^{\frac{1}{2}}$ satisfying $y_0 \le Y$ and $z_0 \le Z$.

Fix some integers m and t. Define the polynomials

$$\begin{aligned} g_{i,j} &= y^j (eM)^i f_{eM}^{m-i} \quad \text{for } i = 0, \dots, m;\ j = 0, \dots, i \\ h_{i,j} &= z^j (eM)^i f_{eM}^{m-i} \quad \text{for } i = 0, \dots, m;\ j = 1, \dots, t. \end{aligned}$$

The parameter t has to be optimized as a function of m.

Since all the polynomials have a term $(eM)^i f_{eM}^{m-i}$, all integer linear combinations of the polynomials have the root (y_0, z_0) modulo $(eM)^m$, i.e. they satisfy the first condition of Howgrave-Graham's theorem (in the bivariate case). Let $L(m)$ be the lattice defined by the basis $B(m)$, where the coefficient vectors of $g_{i,j}(yY, zZ)$ and $h_{i,j}(yY, zZ)$ are the basis vectors of $B(m)$ (with the same parameter choices of i and j as before).

In order to fulfill the second condition in Howgrave-Graham's theorem, we have to find vectors in $L(m)$ with norm less than $\frac{(eM)^m}{\sqrt{\dim L(m)}}$. The following lemma states that one can always find two such sufficiently short vectors in $L(m)$ using the L^3-algorithm.

Lemma 12 *Let e, M be as defined in Theorem 11. Suppose $Y = N^\alpha$ and $Z = 3N^{\frac{1}{2}}$. Then the L^3-algorithm finds at least two vectors in $L(M)$ with norm smaller than $\frac{(eM)^m}{\sqrt{\dim L(m)}}$.*

Proof. Set $n = \dim L(M)$. Applying Theorem 4, we know that the second-to-shortest vector v_2' of an L_3-reduced base satisfies $\|v_2'\| \le 2^{\frac{n}{4}} \det L(M)^{\frac{1}{n-1}}$. Thus, we have to satisfy the condition

$$2^{\frac{n}{4}} \det L(M)^{\frac{1}{n-1}} < \frac{(eM)^m}{\sqrt{n}}.$$

Neglecting all terms that do not depend on N, the condition simplifies to $\det L(M) < (eM)^{m(n-1)}$. We set $t = \tau m$. Then, a straightforward calculation shows that

$$\det L(M) = \left((eMX)^{3\tau+2} Z^{3\tau^2+3\tau+1} \right)^{\frac{1}{6}m^3(1+o(1))}$$

If we plug in the bounds $Y = N^\alpha$ and $Z = 3N^{\frac{1}{2}}$, we obtain the new condition

$$N^{\frac{1}{12}m^3(3\tau^2+3\tau(2\alpha+1)+4\alpha+1)(1+o(1))} \le (eM)^{m(n-1)-(3\tau+2)(\frac{1}{6}m^3(1+o(1)))}$$

On the other hand, we know that $eM \geq N^{\alpha+\frac{1}{6}+\frac{1}{3}\sqrt{1+6\alpha}+\epsilon}$. An easy computation shows that $n = (\tau + \frac{1}{2})m^2$. Again neglecting all low order, we obtain the new condition

$$9\tau^2 + 6(\alpha+\tau) - 2\sqrt{1+6\alpha}(1+3\tau) + 2 \leq 0$$

The left-hand side is minimized for the parameter choice $\tau = \frac{1}{3}(\sqrt{1+6\alpha}-1)$. For this setting of τ, our condition is satisfied. This concludes the proof of Lemma 12.

Combining Theorem 7 and Lemma 12, we obtain two polynomials $f_1(y,z)$, $f_2(y,z)$ with the common root (y_0, z_0) over the integers. By Assumption 5, the resultant $\mathrm{res}_y(f_1, f_2)$ is non-zero such that we can find $z_0 = p + q - 1$ using standard root finding algorithms. This gives us the factorization of N.

Acknowledgement: We want to thank Jean-Pierre Seifert for suggesting to look at partial key exposure attacks on CRT-variants of RSA.

References

1. D. Bleichenbacher, "On the Security of the KMOV public key cryptosystem", Advances in Cryptology - Crypto '97, Lecture Notes in Computer Science vol. 1294. Springer-Verlag, pp. 235–248, 1997
2. J. Blömer, "Closest vectors, successive minima, and dual HKZ-bases of lattices", Proc. of 17th ICALP, Lecture Notes in Computer Science 1853, pp. 248–259, 2000.
3. D. Boneh, G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$", IEEE Trans. on Information Theory vol. 46(4), 2000
4. D. Boneh, G. Durfee, Y. Frankel, "An attack on RSA given a small fraction of the private key bits", Advances in Cryptology - AsiaCrypt '98, Lecture Notes in Computer Science vol. 1514, Springer-Verlag, pp. 25–34, 1998
5. D. Boneh, G. Durfee, Y. Frankel, "Exposing an RSA Private Key Given a Small Fraction of its Bits", Full version of the work from Asiacrypt'98, available at `http://crypto.stanford.edu/~dabo/abstracts/bits_of_d.html`, 1998
6. D. Boneh, R. DeMillo, R. Lipton, "On the importance of checking cryptographic protocols for faults", Advances in Cryptology - Eurocrypt'97, Lecture Notes in Computer Science vol. 1233, Springer-Verlag, pp. 37–51, 1997.
7. H. Cohen, "A Course in Computational Algebraic Number Theory", Springer-Verlag, 1996
8. D. Coppersmith, "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities", Journal of Cryptology 10(4), 1997
9. J. F. Dhem, F. Koeune, P. A. Leroux, P. Mestre, J. J. Quisquater, and J. L. Willems, "A practical implementation of the timing attack", In Proc. of CARDIS 98 – Third smart card research and advanced application conference, 1998
10. G. Durfee, P. Nguyen, "Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99", Advances in Cryptology - Asiacrypt 2000, Lecture Notes in Computer Science vol. 1976, Springer, pp. 14–29, 2000
11. M. Gruber, C.G. Lekkerkerker, "Geometry of Numbers", North-Holland, 1987
12. N. Howgrave-Graham, "Finding small roots of univariate modular equations revisited", Proc. of Cryptography and Coding, Lecture Notes in Computer Science 1355, Springer-Verlag, 1997

13. N. Howgrave-Graham, "Approximate Integer Common Divisors", CaLC 2001, Lecture Notes in Computer Science vol. 2146, pp. 51–66, 2001
14. C. Jutla, "On finding small solutions of modular multivariate polynomial equations", Advances in Cryptology - Eurocrypt '98, Lecture Notes in Computer Science vol. 1403, pp. 158–170, 1998
15. P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems", Advances in Cryptology - Crypto '96, Lecture Notes in Computer Science vol. 1109, pp. 104–113, 1996
16. P. Kocher, J. Jaffe and B. Jun, "Differential power analysis", Advances in Cryptology – CRYPTO '99, Lecture Notes in Computer Science vol. 1666, pp. 388–397, 1999
17. A. Lenstra, H. Lenstra and L. Lovász, "Factoring polynomials with rational coefficients", Mathematische Annalen, 1982
18. L. Lovász, "An Algorithmic Theory of Numbers, Graphs and Convexity", Conference Series in Applied Mathematics, SIAM, 1986
19. V. Shoup, NTL: A Library for doing Number Theory, online available at http://www.shoup.net/ntl/index.html
20. T. Takagi, "Fast RSA-Type Cryptosystem Modulo $p^k q$", Advances in Cryptology - Crypto '98, Lecture Notes in Computer Science vol. 1462, pp. 318–326, 1998
21. J.-J. Quisquater, C. Couvreur, "Fast decipherment algorithm for RSA public-key cryptosystem", Electronic Letters 18, pp. 905–907, 1982