Secret Exponent Attacks on RSA-type Schemes with Moduli $N = p^r q$

Alexander May

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

Abstract. We consider RSA-type schemes with modulus $N = p^r q$ for $r \geq 2$. We present two new attacks for small secret exponent d. Both approaches are applications of Coppersmith's method for solving modular univariate polynomial equations [5]. From these new attacks we directly derive partial key exposure attacks, i.e. attacks when the secret exponent is not necessarily small but when a fraction of the secret key bits is known to the attacker. Interestingly, all of these attacks work for public exponents e of arbitrary size. Additionally, we present partial key exposure attacks for the value $d_p = d \bmod p-1$ which is used in CRT-variants like Takagi's scheme [11]. Our results show that RSA-type schemes that use moduli of the form $N = p^r q$ are more susceptible to attacks that leak bits of the secret key than the original RSA scheme.

Keywords: $N = p^r q$, Coppersmith's method, Partial Key Exposure Attacks

1 Introduction

We investigate attacks on cryptographic schemes that use public moduli of the form $N = p^r q$ for some constant $r > 1$. Moduli of this type have recently been used in different cryptographic designs. Fujioke, Okamoto and Uchiyama [6] presented an electronic cash scheme using a modulus $N = p^2 q$. Furthermore, Okamoto and Uchiyama [10] designed an elegant public-key crypto scheme that is provably as secure as factoring a modulus $N = p^2 q$. A fast CRT-RSA variant using moduli of the form $N = p^r q$ was introduced by Takagi [11] in 1998. The larger one chooses r in Takagi's scheme, the more efficient is the scheme for a fixed bit-size of the modulus N.

Consider an RSA-type scheme with public key (N, e), where $N = p^r q$ for some fixed $r > 1$ and p, q are of the same bit-size. The secret key d satisfies $ed = 1 \bmod \phi(N)$, where $\phi(N)$ is Euler's totient function. We denote by $\mathbb{Z}^*_{\phi(N)}$ the multiplicative group of invertible integers modulo $\phi(N)$.

In 1999, Boneh, Durfee and Howgrave-Graham [3] showed that schemes with moduli of the form $N = p^r q$ are more susceptible to attacks that leak bits of p than the original RSA-scheme. Using Coppersmith's method for solving univariate modular equations [5], they showed that it suffices to know a fraction of $\frac{1}{r+1}$ of the MSBs of p to factor the modulus. It is an interesting task, whether schemes with $N = p^r q$ are also more susceptible to attacks that leak bits of the secret exponent d. In most side-channel attack scenarios (see for instance [7, 8]), it is more reasonable to assume that an adversary gains knowledge of a fraction of the secret key bits than knowledge of the prime factor bits.

Intuitively, one should expect that crypto-systems with moduli of the form $N = p^r q$, $r > 1$ are more vulnerable to secret key attacks than the original RSA-scheme, since for a fixed bit-size of N the amount of secret information encoded in the prime factors is smaller than in RSA. Hence, these schemes should be more susceptible to small secret key attacks like the Wiener attack [12] and the Boneh-Durfee attack [1]. Likewise, these schemes should be more susceptible to so-called partial key exposure attacks that use the knowledge of a fraction of the secret key bits like the Boneh-Durfee-Frankel attack [2] and the Blömer-May attack [4].

In contrast to this intuition, it was stated in the work of Takagi [11] that RSA-type schemes with $N = p^r q$ seem to be less vulnerable to attacks for small decryption exponents d than the original RSA-scheme. Namely, Takagi showed a generalized Wiener-bound of $d \leq N^{\frac{1}{2(r+1)}}$. However, we introduce two attacks with improved bounds for the size of d. Both new attacks are applications of Coppersmith's method for solving modular univariate polynomial equations [5].

Our first attack directly uses the results of Boneh, Durfee and Howgrave-Graham [2] for factoring $N = p^r q$. It yields an improved bound of

$$d \leq N^{\frac{r}{(r+1)^2}} \quad \text{for } r \geq 2.$$

Let us compare the results for $r = 2$: Takagi requires that $d \leq N^{\frac{1}{6}}$ whereas our new method works whenever $d \leq N^{\frac{2}{9}}$.

Our second method makes use of Coppersmith's method in the univariate case and leads to the bound

$$d \leq N^{\left(\frac{r-1}{r+1}\right)^2} = N^{1-\frac{4r}{(r+1)^2}} \quad \text{for } r \geq 2.$$

Interestingly in contrast to the previous bounds, this new bound converges to N for growing r instead of converging to 1. It improves upon our first attack for all parameter choices $r \geq 3$: The second attack requires that $d \leq N^{\frac{1}{4}}$ in the case $r = 3$ compared to $d \leq N^{\frac{3}{16}}$ for our first method. Thus, our first attack is only superior to the other methods in the case $r = 2$. On the other hand, moduli of the form $N = p^2 q$ are frequently used in cryptography and therefore they represent one of the most important cases.

Interestingly, the new attacks for small decryption exponents d have two new features which the original Wiener attack and the Boneh-Durfee attack do not possess:

- One cannot counteract the new attacks by choosing large public exponents e, since the attacks are independent of the value of e. In comparison, the Wiener bound $d \leq N^{\frac{1}{4}}$ and the Boneh-Durfee bound $d \leq N^{0.292}$ require

that $e < \phi(N)$. It is known that the attacks cannot be applied for any size of d if $e > N^{1.5}$ or $e > N^{1.875}$, respectively.
– The new attacks immediately imply a partial key exposure attack for d with known most significant bits (MSBs). Namely, it makes no difference in the attacks whether the most significant bits of d are zero (and thus d is a small decryption exponent) or are known to the attacker. In contrast, Wiener's attack and the Boneh-Durfee attack for small decryption exponents do not work when the MSB's are non-zero but known. In addition, the new attacks also provide partial key exposure attacks for known least significant bits (LSBs).

Using the first attack, we are able to prove that a fraction of

$$1 - \frac{r}{(r+1)^2} \text{ of the MSBs } \mathit{or} \text{ LSBs of } d$$

suffice to find the factorization of $N = p^r q$. The second attack yields partial key exposure attacks that require only a fraction of

$$\frac{4r}{(r+1)^2} \text{ of the MSBs } \mathit{or} \text{ LSBs of } d$$

in order to factor N.

The resulting partial key exposure attacks share the same property as the underlying attacks for small decryption exponents d: They do not rely on the size of the public exponent e. Note that all partial key exposure attacks mentioned in the literature [2, 4] are dependent on e and do not work for arbitrary $e \in \mathbb{Z}^*_{\phi(N)}$. The new methods are the first partial key exposure attacks that work for all public exponents e.

The reason that all former attacks on RSA-type schemes depend on the size of e is that they all compute the parameter k in the RSA key equation $ed - 1 = k\phi(N)$. In contrast, our new attacks do not require the computation of k. Thus, k must not be a small parameter and hence the parameters e and d can be increased (thereby increasing k) without affecting the usability of the attacks.

The reason that our new attacks do not require the direct computation of k is mainly that for moduli $N = p^r q$ the group order of the multiplicative group Z_N^* is $\phi(N) = p^{r-1}(p-1)(q-1)$. Thus for $r \geq 2$, $\phi(N)$ and N share the common divisors p and p^{r-1}, respectively, and this can be used in the attacks by constructing polynomials with small roots modulo p (our first attack) and modulo p^{r-1} (our second attack), respectively. But looking at the equation $ed-1 = k\phi(N)$ modulo p (respectively modulo p^{r-1}) removes the unknown parameter k.

We want to point out that these new attacks are normally not a threat to Takagi's scheme [11]. Since Takagi's CRT-decryption process only makes use of the values $d_p = d \bmod p - 1$ and $d_q = d \bmod q - 1$, it suffices to choose an d which satisfies $ed = 1 \bmod (p-1)(q-1)$. For this kind of public-key/secret-key pair (e, d), our previous attacks do not apply. Even worse, normally one would not even store the value of d but only the values of d_p and d_q for the decryption process. Therefore, it is reasonable to assume that an attacker may only get bits of d_p or d_q. Hence, it is an interesting task to derive partial key exposure attacks for known bits of d_p (respectively d_q).

We show that the partial key exposure attacks of Blömer and May [4] for moduli $N = pq$ generalize to the case $N = p^r q$. Interestingly, the results are again much better for $r > 1$. Namely, we present attacks that need only a fraction of

$$\frac{1}{r+1} \text{ of the MSBs } \mathit{or} \text{ LSBs of } d_p$$

when the public exponent e is small. This shows that Takagi's scheme is also more susceptible to attacks that leak bits of d_p than normal CRT-RSA.

The paper is organized as follows: In Section 2, we review Coppersmith's method for modular univariate polynomial equations [5]. Here, we introduce a reformulation of Coppersmith's orginal theorem that unifies all known applications (see [2–5]) of the method in the univariate case. As an example, we derive the result of Boneh, Durfee and Howgrave-Graham [3] for factoring $N = p^r q$ as a direct application of Coppersmith's theorem. The first attack for small d and the corresponding partial key exposure attacks are presented in Section 3. In Section 4, we describe our second attack. The partial key exposure attacks for d_p are presented in Section 5.

2 Coppersmith's method and the result of BDH

Let us recall Coppersmith's theorem for solving modular univariate polynomial equations [5]. Here, we give the theorem in a slightly more general form than originally stated. However, one can prove the theorem in a completely analogous way to the reasoning in the original proof of Coppersmith. We give the details of the proof in the full version of the paper.

Theorem 1 (Coppersmith) *Let N be an integer of unknown factorization, which has a divisor $b \geq N^{\beta}$. Let $f_b(x)$ be an univariate, monic polynomial of degree δ. Furthermore, let c_N be a function that is upper-bounded by a polynomial in $\log N$. Then we can find all solutions x_0 for the equation $f_b(x) = 0 \bmod b$ with*

$$|x_0| \leq c_N N^{\frac{\beta^2}{\delta}}$$

in time polynomial in $(\log N, \delta)$.

Coppermith formulated Theorem 1 for the special case where $N = b$. Then the bound for the solutions becomes $|x_0| \leq c_N N^{\frac{1}{\delta}}$. However, the above formulation of Coppersmith's theorem has some advantages: For instance, it is not hard to see that the result of Boneh, Durfee and Howgrave-Graham [3] for factoring $N = p^r q$ with known bits is a direct application of Theorem 1 using the polynomial $f_{p^r}(x) = (x + \tilde{p})^r$.

In fact, the following theorem is stated in the original work of Boneh, Durfee and Howgrave-Graham for the special case $k = 1$, but we formulate it in a slightly more general way, since we will use this generalization in Section 3.

Theorem 2 (BDH) *Let $N = p^r q$, where r is a known constant and p, q are of the same bit-size. Let k be an (unknown) integer that is not a multiple of $p^{r-1}q$. Suppose we know an integer $\tilde{p}$ with*

$$|\, kp - \tilde{p}\,| \leq N^{\frac{r}{(r+1)^2}}.$$

Then N can be factored in polynomial time.

Let us interpret the result of Theorem 2. In order to factor N it suffices to find an integer $\tilde{p}$ which is within the range $N^{\frac{r}{(r+1)^2}}$ of some multiple of p (which is not a multiple of N). In the following section, we present our first new attack that constructs an integer $\tilde{p}$ with the above property whenever d is sufficiently small.

3 The attack modulo p

We present our first attack for small decryption exponents d and afterwards extend this approach to partial key exposure attacks.

Theorem 3 *Let $N = p^r q$, where $r \geq 2$ is a known constant and p, q are primes of the same bit-size. Let $(e, d) \in \mathbb{Z} \times \mathbb{Z}^*_{\phi(N)}$ be the public-key/secret-key pair satisfying $ed = 1 \bmod \phi(N)$. Suppose that*

$$d \leq N^{\frac{r}{(r+1)^2}}.$$

Then N can be factored in probabilistic polynomial time.

Proof: We know that $\phi(N) = p^{r-1}(p-1)(q-1)$ and therefore the key pair (e, d) satisfies the equation

$$ed - 1 = kp^{r-1}(p-1)(q-1) \quad \text{for some } k \in \mathbb{N}. \tag{1}$$

Let E be the inverse of e modulo N, i.e. $Ee = 1 + cN$ for some $c \in \mathbb{N}$. If E does not exist then $\gcd(e, N)$ must be a non-trivial divisor of N.

Note that each possible non-trivial divisor p^s, $p^s q$ or q $(1 \leq s \leq r)$ does immediately yield the complete factorization of N: p^s can be easily factored by guessing s and taking the s^{th} root over the integers. On the other hand, $p^s q$ yields $\frac{N}{p^s q} = p^{r-s}$ which reduces this case to the previous one. Similarly, q gives us p^r.

Hence, let us assume wlog that the inverse E of e modulo N exists. Multiplying equation (1) by E leads to

$$d - E = (Ekp^{r-2}(p-1)(q-1) - cp^{r-1}qd)p.$$

Thus, E is a multiple of p up to an additive error of $d \leq N^{\frac{r}{(r+1)^2}}$. In order to apply Theorem 2, it remains to show that the expression $Ekp^{r-2}(p-1)(q-1) - cp^{r-1}qd$ is not a multiple of $p^{r-1}q$. Since $p^{r-1}q$ divides the second term, this is equivalent to show that $Ek(p-1)(q-1)$ is not a multiple of pq. By assumption, we have $\gcd(E, N) = 1$ and thus it remains to prove that pq does not divide $k(p-1)(q-1)$. Assume $k(p-1)(q-1) = c'pq$ for some $c' \in \mathbb{N}$. Then equation (1) simplifies to

$$ed - 1 = c'N.$$

On the other hand we know that $eE - 1 = cN$. Combining both equalities we obtain that $d = E \bmod N$. Since $d, E < N$ we have $d = E$ even over $\mathbb{Z}$. It is a well-known fact that the knowledge of the secret key d yields the factorization of N in probabilistic polynomial time (see for instance [9], Chapter 4.6.1).

We briefly summarize our factorization algorithm.

(Mod p)-attack for small d using a modulus $N = p^r q$

INPUT: (N, e), where $N = p^r q$ and $ed = 1 \bmod \phi(N)$ for some $d \leq N^{\frac{r}{(r+1)^2}}$.

1. Compute $E = e^{-1} \bmod N$. If the computation of E fails, output p, q.
2. Run the algorithm of Theorem 2 on input E. If the algorithm's output is p, q then EXIT.
3. Otherwise set $d = E$ and run a probabilistic factorization algorithm on input (N, e, d).

OUTPUT: p, q

Since every step of the algorithm runs in (probabilistic) polynomial time, this concludes the proof of the theorem. $\square$

Theorem 3 gives us a polynomial time factoring algorithm whenever a certain amount of the MSBs of d are zero. The following corollary shows how the proof of Theorem 3 can be easily generalized such that the result does not only hold if the MSBs of d are zero but instead if they are known to the attacker. This gives as a partial key exposure attack for known MSBs with an analogous bound.

Corollary 4 *(MSB) Let $N = p^r q$, where $r \geq 2$ is a known constant and p, q are primes of the same bit-size. Let $(e, d) \in \mathbb{Z} \times \mathbb{Z}^*_{\phi(N)}$ be the public-key/secret-key pair satisfying $ed = 1 \bmod \phi(N)$. Given $\tilde{d}$ such that*

$$|\, d - \tilde{d} \,| \leq N^{\frac{r}{(r+1)^2}}.$$

Then N can be factored in probabilistic polynomial time.

Proof: The key-pair (e, d) satisfies the equality

$$e(d - \tilde{d}) + e\tilde{d} - 1 = kp^{r-1}(p-1)(q-1) \quad \text{for some } k \in \mathbb{N}.$$

Let $E = e^{-1} \bmod N$, i.e. $Ee = 1 + cN$ for some $c \in \mathbb{N}$. If E does not exist, we obtain the factorization of N. Multiplying the above equation by E yields

$$(d - \tilde{d}) + E(e\tilde{d} - 1) = (Ekp^{r-2}(p-1)(q-1) - cp^{r-1}q(d - \tilde{d}))p.$$

Thus, $E(e\tilde{d} - 1)$ is a multiple of p up to an additive error of $|d - \tilde{d}| \leq N^{\frac{r}{(r+1)^2}}$. The rest of the proof is completely analogous to the proof of Theorem 3. $\square$

Corollary 4 implies that one has to know roughly a fraction of $1 - \frac{r}{(r+1)^2}$ of the MSBs of d for our partial key exposure attack. We can also derive a partial key exposure attack for known LSBs with an analogous bound.

Corollary 5 *(LSB) Let $N = p^r q$, where $r \geq 2$ is a known constant and p, q are primes of the same bit-size. Let $(e, d) \in \mathbb{Z} \times \mathbb{Z}^*_{\phi(N)}$ be the public-key/secret-key pair satisfying $ed = 1 \bmod \phi(N)$. Given d_0, M with $d = d_0 \bmod M$ and*

$$M \geq N^{1 - \frac{r}{(r+1)^2}}.$$

Then N can be factored in probabilistic polynomial time.

Proof: Let us write $d = d_1 M + d_0$, were the unknown d_1 satisfies $d_1 = \frac{d - d_0}{M} < \frac{N}{M} \leq N^{\frac{r}{(r+1)^2}}$. We have the key equation

$$ed_1 M + ed_0 - 1 = kp^{r-1}(p-1)(q-1) \quad \text{for some } k \in \mathbb{N}.$$

Multiply the equation by $E = (eM)^{-1} \bmod N$. We see that $E(ed_0 - 1)$ is a multiple of p up to an additive error of $|d_1| < N^{\frac{r}{(r+1)^2}}$. The rest of the proof is analogous to the proof of Theorem 3. $\square$

4 Attack modulo p^{r-1}

Our first attack applied Theorem 2 which in turn uses a polynomial with small roots modulo p. In our second attack we will construct a polynomial with a small root modulo p^{r-1} and directly apply Coppersmith's method in the univariate case (Theorem 1). This approach yields better results than the first one whenever $r \geq 3$.

Theorem 6 *Let $N = p^r q$, where $r \geq 2$ is a known constant and p, q are primes of the same bit-size. Let $(e, d) \in \mathbb{Z} \times \mathbb{Z}^*_{\phi(N)}$ be the public-key/secret-key pair satisfying $ed = 1 \bmod \phi(N)$. Suppose that*

$$d \leq N^{\left(\frac{r-1}{r+1}\right)^2}.$$

Then N can be factored in probabilistic polynomial time.

Proof: The key pair (e, d) satisfies the equation

$$ed - 1 = kp^{r-1}(p-1)(q-1) \quad \text{for some } k \in \mathbb{N}.$$

Let E be the inverse of e modulo N, i.e. $Ee = 1 + cN$ for some $c \in N$. In the case that E does not exist, $\gcd(e, N)$ yields the complete factorization of N as shown in the proof of Theorem 3. Multiplying our equation by E leads to

$$d - E = (Ek(p-1)(q-1) - cdpq)p^{r-1}.$$

This gives us a simple univariate polynomial

$$f_{p^{r-1}}(x) = x - E$$

with the root $x_0 = d$ modulo p^{r-1}.

Thus, we have a polynomial $f_{p^{r-1}}$ of degree $\delta = 1$ with a root x_0 modulo p^{r-1}. In order to apply Theorem 1, we have to find a lower bound for p^{r-1} in terms of N.

Since p and q are of the same bit-size, we know that $p \geq \frac{1}{2}q$. Hence $p^{r-1} = \frac{N}{pq} \geq \frac{N}{2p^2}$. This gives us

$$p^{r-1} \geq \left(\frac{1}{2}N\right)^{\frac{r-1}{r+1}} \geq \frac{1}{2}N^{\frac{r-1}{r+1}}.$$

Thus, we can choose $\beta = \frac{r-1}{r+1} - \frac{1}{\log N}$ and apply Theorem 1 with the parameter choice β, δ and $c_N = 4$. We can find all roots x_0 that are in absolute value smaller than

$$4N^{\frac{\beta^2}{\delta}} = 4N^{(\frac{r-1}{r+1})^2 - \frac{2(r-1)}{(r+1)\log N} + \frac{1}{\log^2 N}} \geq 4N^{(\frac{r-1}{r+1})^2 - \frac{2}{\log N}} = N^{(\frac{r-1}{r+1})^2}.$$

Hence, we obtain the value $x_0 = d$. We can run a probabilistic factorization algorithm on input (N, e, d) in order to obtain the factorization of N in expected polynomial time.

Remark 7 *Another (deterministic) polynomial time method to find the factorization of N could be the computation of $\gcd(ed - 1, N)$. Since $ed - 1 = kp^{r-1}(p-1)(q-1)$, the computation yields a non-trivial divisor of N iff pq does not divide $k(p-1)(q-1)$, which is unlikely to happen. As shown in the proof of Theorem 3, a non-trivial divisor of N reveals the complete factorization of the modulus. So in practice, one might try this alternative gcd-method first and if it fails, one applies a probabilistic algorithm on the key-pair (N, e, d).*

Let us summarize our new factorization algorithm.

(Mod p^r)-attack for small d using a modulus $N = p^r q$

INPUT: (N, e), where $N = p^r q$ and $ed = 1 \bmod \phi(N)$ for some $d \leq N^{\left(\frac{r-1}{r+1}\right)^2}$.

1. Compute $E = e^{-1} \bmod N$. If E does not exist, compute $\gcd(e, N)$ and output p, q.
2. Apply the algorithm of Theorem 1 on input N, $f_{p^{r-1}} = x - E$, $\beta = \frac{r-1}{r+1} - \frac{1}{\log N}$ and $c_N = 2$. This gives us the value d.
3. If the computation $\gcd(ed - 1, N)$ yields the factorization, EXIT.
4. Run a probabilistic factorization algorithm on input (N, e, d).

OUTPUT: p, q

Every step of the algorithm can be computed in probabilistic polynomial time, which concludes the proof of Theorem 6 $\square$

Similar to the first attack (the (Mod p)-attack) for small decryption exponent d, we can also easily derive partial key exposure attacks for the new attack of Theorem 6. The proof of Theorem 6 shows that in order to find the factorization of N, it suffice to find a linear, univariate polynomial $f_{p^{r-1}}(x) = x + c$ with a root $x_0, |x_0| \leq N^{\left(\frac{r-1}{r+1}\right)^2}$ modulo p^{r-1}.

We will show that this requirement is satisfied in the following partial key exposure attacks. Instead of using small decryption exponents $d < N^{\left(\frac{r-1}{r+1}\right)^2} = N^{1-\frac{4r}{(r+1)^2}}$, the attacker has to know a fraction of roughly $\frac{4r}{(r+1)^2}$ of the bits of N in order to succeed.

Corollary 8 *(MSB) Let $N = p^r q$, where $r \geq 2$ is a known constant and p, q are primes of the same bit-size. Let $(e, d) \in \mathbb{Z} \times \mathbb{Z}^*_{\phi(N)}$ be the public-key/secret-key pair satisfying $ed = 1 \bmod \phi(N)$. Given $\tilde{d}$ with*

$$| \, d - \tilde{d} \, | \leq N^{\left(\frac{r-1}{r+1}\right)^2}.$$

Then N can be factored in probabilistic polynomial time.

Proof: We know that

$$e(d - \tilde{d}) + e\tilde{d} - 1 = 0 \bmod \phi(N),$$

and $\phi(N)$ is a multiple of p^{r-1}. Multiply the equation by $E = e^{-1} \bmod N$, which gives us the desired linear polynomial

$$f_{p^{r-1}}(x) = x + E(e\tilde{d} - 1)$$

with the small root $x_0 = d - \tilde{d}$, $|x_0| \leq N^{\left(\frac{r-1}{r+1}\right)^2}$ modulo p^{r-1}. The rest of the proof is analogous to the proof of Theorem 6. $\square$

In a similar fashion, we derive a partial key exposure attack for known LSBs.

Corollary 9 *(LSB) Let $N = p^r q$, where $r \geq 2$ is a known constant and p, q are primes of the same bit-size. Let $(e, d) \in \mathbb{Z} \times \mathbb{Z}^*_{\phi(N)}$ be the public-key/secret-key pair satisfying $ed = 1 \bmod \phi(N)$. Given d_0, M with $d = d_0 \bmod M$ and*

$$M \geq N^{\frac{4}{(r+1)^2}}.$$

Then N can be factored in probabilistic polynomial time.

Proof: Let us write $d = d_1 M + d_0$. Then the unknown parameter satisfies $d_1 < \frac{N}{M} \leq N^{\left(\frac{r-1}{r+1}\right)^2}$. For the key-pair (e, d) we have

$$e(d_1 M + d_0) - 1 = 0 \bmod \phi(N),$$

where $\phi(N)$ is a multiple of p^{r-1}. Multiplying this equation by $E = (eM)^{-1}$ modulo N gives us the desired linear polynomial

$$f_{p^{r-1}}(x) = x + E(ed_0 - 1)$$

with the small root d_1 modulo p^{r-1}. The rest of the proof is analogous to the proof of Theorem 6. $\square$

5 Partial Key Exposure Attacks for $d_p = d$ modulo $p - 1$

The partial key exposure attacks that we consider in this section for moduli $N = p^r q$ can be considered as a generalization of the results of Blömer and May [4]. The attacks are an application of the theorem of Boneh, Durfee and Howgrave-Graham (Theorem 2).

We derive simple partial key exposure attacks for small public exponents e in both cases: known MSBs and known LSBs. The new attacks are a threat to schemes that use CRT-decoding (for instance Takagi's scheme [11]) in combination with small public exponents.

Let us state our LSB-attack.

Theorem 10 *Let $N = p^r q$, where $r \geq 1$ is a known constant and p, q are primes of the same bit-size. Let e be the public key and let d_p satisfy $ed_p = 1 \bmod p - 1$. Given d_0, M with $d_0 = d_p \bmod M$ and*

$$M \geq 2N^{\frac{1}{(r+1)^2}}.$$

Then N can be factored in time $e \cdot poly(\log(N))$.

Proof: Let us consider the RSA key equation

$$ed_p - 1 = k(p-1) \quad \text{for some } k \in \mathbb{Z}.$$

Since $d_p < (p-1)$, we obtain the inequality $k < e$. Let us write $d_p = d_1 M + d_0$. We can bound the unknown d_1 by $d_1 < \frac{p}{M} \le N^{\frac{r}{(r+1)^2}}$. Our equation above can be rewritten as

$$ed_1 M + ed_0 + k - 1 = kp.$$

Compute the inverse E of eM modulo N, i.e. $EeM = 1 + cN$ for some $c \in \mathbb{N}$. If E does not exist, we obtain from $\gcd(eM, N)$ the complete factorization of N as shown in Theorem 3. Multiplying our equation with E leaves us with

$$d_1 + E(ed_0 + k - 1) = (Ek - cp^{r-1}qd_1)p.$$

Thus, $E(ed_0 + k - 1)$ is a multiple of p up to some additive error $d_1 \le N^{\frac{r}{(r+1)^2}}$. Since the parameter k is unknown, we have to do a brute force search for k in the interval $[1, e)$. In order to apply Theorem 2, it remains to show that the term $(Ek - cp^{r-1}qd_1)$ is not a multiple of $p^{r-1}q$. This is equivalent to the condition that $p^{r-1}q$ does not divide Ek, but we know that $\gcd(E, N) = 1$ and thus $p^{r-1}q$ must not divide k. But $p^{r-1}q$ cannot divide k in the case $e \le p^{r-1}q$ and otherwise we can easily check the condition by computing $\gcd(k, N)$ for every possible k. The algorithm of Theorem 2 yields the factorization of N for the correct guess of k.

We briefly summarize our factorization algorithm.

Algorithm LSB-Attack for d_p and moduli $N = p^r q$

INPUT: – (N, e), where $N = p^r q$ and d_p satisfies $ed_p = 1 \bmod p-1$
– d_0, M with $d_0 = d_p \bmod M$ and $M \ge 2N^{\frac{1}{(r+1)^2}}$

1. Compute $E = (eM)^{-1} \bmod N$. If the computation of E fails, find the factors p, q of N using $\gcd(eM, N)$.
2. FOR $k = 1$ TO e
   (a) If $\gcd(k, N) > 1$ find the factors p, q.
   (b) Run the algorithm of Theorem 2 on input $E(ed_0 + k - 1)$. If the algorithm's output is p, q then EXIT.

OUTPUT: p, q

The running time of the algorithm is $e \cdot \mathrm{poly}(\log N)$, which concludes the proof. □

Note that our method from Theorem 10 is polynomial time for public exponents of the size $\mathrm{poly}(\log(N))$ and requires only a $\frac{1}{(r+1)^2}$-fraction of the bits (in terms of the size of N), which is a $\frac{1}{r+1}$-fraction of the bits of d_p. The following theorem gives us a similar result for partial key exposure attacks with known MSBs, but in contrast the method is polynomial time for all public exponents $e < N^{\frac{r}{(r+1)^2}}$.

We show that an approximation of d_p up to $N^{\frac{r}{(r+1)^2}-\alpha}$ suffices to find the factorization of N. Note that d_p is of size roughly $N^{\frac{1}{r+1}}$. Hence in the case $\alpha = 0$, a fraction of $\frac{1}{r+1} - \frac{r}{(r+1)^2} = \frac{1}{(r+1)^2}$ of the bits is enough (in terms of the size of N).

Theorem 11 *Let $N = p^r q$, where $r \geq 1$ is a known constant and p, q are primes of the same bit-size. Let $e = N^\alpha$, $\alpha \in [0, \frac{r}{(r+1)^2}]$ be the public key and let d_p satisfy $ed_p = 1 \bmod p-1$. Given $\tilde{d}$ with*

$$| \, d_p - \tilde{d} \, | \leq N^{\frac{r}{(r+1)^2}-\alpha}.$$

Then N can be factored in polynomial time.

Proof: We know that

$$ed_p - 1 = k(p-1) \quad \text{for some } k \in \mathbb{N},$$

with $k < e$. The term $e\tilde{d}$ is an approximation of kp up to an additive error of

$$|kp - e\tilde{d}| = |e(d_p - \tilde{d}) + k - 1| \leq |e(d_p - \tilde{d})| + |k-1|$$

$$\leq N^{\frac{r}{(r+1)^2}} + N^\alpha \leq 2N^{\frac{r}{(r+1)^2}}.$$

Thus, one of the terms $e\tilde{d} \pm N^{\frac{r}{(r+1)^2}}$ satisfies the bound of Theorem 2. Note that the algorithm of Theorem 2 can be applied since $k < e < N^{\frac{r}{(r+1)^2}}$ and thus k cannot be a multiple of $p^{r-1}q = \Omega(N^{\frac{r}{r+1}})$.

Let us briefly summarize the factorization algorithm.

MSB-Attack for d_p and moduli $N = p^r q$

INPUT: – (N, e), where $N = p^r q$ and d_p satisfies $ed_p = 1 \bmod p-1$
– $\tilde{d}$ with $|d_p - \tilde{d}| \leq N^{\frac{r}{(r+1)^2}-\alpha}$, where $\alpha = \log_N(e)$.

1. Compute $\tilde{p} = e\tilde{d}$.
2. Run the algorithm of Theorem 2 on input $\tilde{p} + N^{\frac{r}{(r+1)^2}}$. If the algorithm's output is p, q then EXIT.
3. Otherwise run the algorithm of Theorem 2 on input $\tilde{p} - N^{\frac{r}{(r+1)^2}}$.

OUTPUT: p, q

The algorithm runs in time polynomial in $\log(N)$, which concludes the proof. $\square$

References

1. 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
2. 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
3. D. Boneh, G. Durfee, and N. Howgrave-Graham, "Factoring $N = p^r q$ for large r", Advances in Cryptology - Crypto '99, Lecture Notes in Computer Science Vol. 1666, Springer-Verlag, pp. 326–337, 1999
4. J. Blömer, A. May, "New Partial Key Exposure Attacks on RSA", Advances in Cryptology - Crypto 2003, Lecture Notes in Computer Science Vol. 2729, pp. 27–43, Springer Verlag, 2003
5. D. Coppersmith, "Small solutions to polynomial equations and low exponent vulnerabilities", Journal of Cryptology, Vol. 10(4), pp. 223–260, 1997.
6. A. Fujioke, T. Okamoto, Miyaguchi, "ESIGN: An Efficient Digital Signature Implementation for Smartcards", Advances in Cryptology - Eurocrypt '91, Lecture Notes in Computer Science Vol. 547, Springer Verlag, pp. 446-457, 1991
7. 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, Springer Verlag, pp. 104–113, 1996
8. P. Kocher, J. Jaffe and B. Jun, "Differential power analysis", Advances in Cryptology – Crypto '99, Lecture Notes in Computer Science Vol. 1666, Springer Verlag, pp. 388–397, 1999
9. D. Stinson, "Cryptography Theory and Practice", Second Edition, CRC Press, 2002
10. T. Okamoto, S. Uchiyama, "A new public key cryptosystem as secure as factoring", Advances in Cryptology - Eurocrypt '98, Lecture Notes in Computer Science Vol. 1403, Springer Verlag, pp. 308–318, 1998
11. T. Takagi, "Fast RSA-type cryptosystem modulo $p^k q$", Advances in Cryptology - Crypto '98, Lecture Notes in Computer Science Vol. 1462,Springer-Verlag, pp.318–326, 1998
12. M. Wiener, "Cryptanalysis of short RSA secret exponents", IEEE Transactions on Information Theory, Vol. 36, pp. 553–558, 1998.