0

Diophantine and Lattice Cryptanalysis of the RSA Cryptosystem

Abderrahmane Nitaj
Laboratoire de Mathématiques Nicolas Oresme, Université de Caen
France

1. Introduction

The work done by Alan Turing brought computer science and cryptography into the modern world. Then, within a few decades, cryptography has evolved from a branch of mathematics into a self-contained field of science. Basically, there are two types of cryptography: symmetric-key cryptography and public-key cryptography. The concept of the public-key cryptosystem was proposed by Diffie and Hellman (Diffie & Hellman, 1976) in 1976. Since then, a number of public-key cryptosystems have been proposed to realize the notion of public-key cryptosystems. The RSA public-key cryptosystem was invented by Rivest, Shamir, and Adleman (Rivest et al., 1978) in 1978. These days the RSA system is the best known and most widely accepted public key cryptosystem. RSA is most commonly used for providing privacy and ensuring authenticity of digital data. It is used in several operating systems, like Microsoft, Apple and Sun. It is also used for securing web traffic, e-mail and smart cards. Hence, many practical issues have been considered when implementing RSA in order to reduce the encryption or the execution decryption time.

The mathematical operations in RSA depend on three parameters, the modulus $N = pq$ which is the product of two large primes p and q, the public exponent e and the private exponent d, related by the congruence $ed \equiv 1 \pmod{(p-1)(q-1)}$. The encryption and decryption in RSA require taking heavy exponential multiplications modulus the large integer $N = pq$. To reduce the encryption time, one may wish to use a small public exponent e. On the other hand, to reduce the decryption time, one may also be tempted to use a short secret exponent d. The choice of a small d is especially interesting when the device performing secret operations has limited power. In 1990, Wiener (Wiener, 1990) presented an attack on RSA with short secret exponent, called continued fraction attack. He used Diophantine approximations to show that if $d < N^{0.25}$, then it easy to recover d, p and q making RSA totally insecure.

In 1996, Coppersmith (Coppersmith, 1997) introduced two methods for finding small roots of polynomial equations using lattice reduction, one for the univariate modular case and another one for the bivariate case over the integers. His method is based on lattice-reduction techniques. Since then, many cryptanalytic applications have been based on these methods, for example the factorization of $N = pq$ knowing a fraction of the most significant bits on each factor. Another well-known example is the cryptanalysis of RSA with small private key. In 1999, based on the seminal work of Coppersmith, Boneh and Durfee (Boneh & Durfee, 1999) presented an attack on RSA which recovers p and q if $d < N^{0.292}$.

In this chapter, we present the diophantine and the lattice techniques used in the cryptanalysis of RSA as well as the most powerful attacks on RSA using these techniques. The first part is devoted to the diophantine approximations and their applications to RSA, namely some generalizations of Wiener's method. The second part presents the lattice-reduction methods and related attacks on RSA. The third part presents some attacks combining the diophantine approximations and the lattice-reduction techniques.

2. The RSA Cryptosystem

We review the basic RSA public key system. We describe five constituent algorithms: key generation, encryption, decryption, signature and signature verification. The key generation algorithm takes a security parameter k as input. The algorithm generates two $(k/2)$-bit primes, p and q, and sets $N = pq$. Popular parameters are $k = 1024$ and $k = 2048$. The large number N is called the RSA modulus and the number $\phi(N) = (p-1)(q-1)$ is the Euler totient function. Next, the algorithm picks some value e satisfying $\gcd(e, \phi(N)) = 1$ and computes d such that $ed \equiv 1 \pmod{\phi(N)}$ and $d < \phi(N)$. The pair (N, e) is called the public key and (N, d) is the private key. The value e is called the public exponent while d is the private exponent. To encrypt a message using an RSA public key (N, e), one first transforms the message to obtain a positive integer M with $M < N$. The encrypted text is then computed as $C \equiv M^e \pmod{N}$. To decrypt an encrypted message C using the private key (N, d), one simply computes $M \equiv C^d \pmod{N}$. An encrypted message C can be digitally signed by applying the decryption operation $S \equiv C^d \pmod{N}$. The digital signature can then be verified by applying the encryption operation $C \equiv S^e \pmod{N}$. To show that the decrypting function inverts the encryption function, rewrite $ed \equiv 1 \pmod{\phi(N)}$ as an equation $ed = 1 + k\phi(N)$ for some positive integer k. A well known of Euler (see e.g. (Hardy & Wright, 1965), Theorem 72) says that $M^{\phi(N)} \equiv 1 \pmod{N}$ if $\gcd(M, N) = 1$. Hence

$$C^e \equiv M^{ed} \equiv M^{1+k\phi(N)} \equiv M \cdot M^{k\phi(N)} \equiv M \cdot \left(M^{\phi(N)}\right)^k \equiv M \pmod{N}.$$

Below we describe in detail the initial schemes of the RSA Cryptosystem.

- **RSA Key Generation**
  INPUT: The bitsize k of the modulus.
  OUTPUT: A public key (N, e) and a private key (N, d).

  1. Generate two large random and distinct $(k/2)$-bit primes p and q.
  2. Compute $N = pq$ and $\phi(N) = (p-1)(q-1)$.
  3. Choose a random integer e such that $3 \leq e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$.
  4. Compute the unique integer d such that $1 \leq e < \phi(N)$ and $ed \equiv 1 \pmod{\phi(N)}$.
  5. Return the public key (N, e) and the private key (N, d).

- **RSA Encryption**
  INPUT: The public key (N, e) and the plaintext $\mathbf{m}$.
  OUTPUT: The ciphertext C.

  1. Represent the message $\mathbf{m}$ as an integer M with $1 \leq M \leq N-1$.
  2. Compute $C \equiv M^e \pmod{N}$.

3. Return the ciphertext C.

- **RSA Decryption**
  INPUT: The private key (N, d) and the the ciphertext C.
  OUTPUT: The message $\mathbf{m}$.

  1. Compute $M \equiv C^d \pmod{N}$.
  2. Transform the number M to the message $\mathbf{m}$.
  3. Return the message $\mathbf{m}$.

3. Diophantine Approximations

3.1 Background on continued fractions

The theory of Diophantine approximations, named after Diophantus of Alexandria, deals with the approximation of real numbers by rational numbers. This can be achieved by continued fractions. Continued fractions have many properties and applications in Number Theory and cryptographic problems. They are used to find good Diophantine approximations to rational and irrational numbers, to solve diophantine equations and to build attacks on some instances of RSA. In this section, we examine the basic properties of continued fractions.

Definition 3.1 (Continued Fraction Expansion)**.** A continued fraction is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_m + \ddots}}} = [a_0, a_1, \ldots, a_m, \ldots],$$

where a_0 is an integer and a_n are positive integers for $n \geq 1$. The a_n are called the partial quotients of the continued fraction.

It is clear that every finite continued fraction defines a rational number. Conversely, every real number $x \neq 0$ can be expanded as a finite or infinite continued fraction by the continued fraction algorithm as follows. Let $\lfloor x \rfloor$ denote the greatest integer less than or equal to x. Let $x_0 = x$ and $a_0 = \lfloor x_0 \rfloor$. Then, for $i \geq 0$, define

$$x_{i+1} = \frac{1}{x_i - a_i}, \quad a_{i+1} = \lfloor x_{i+1} \rfloor.$$

The procedure terminates only if $a_i = x_i$ for some $i \geq 0$, that is if x is a rational number.
The continued fraction of a rational number $x = \frac{a}{b}$ with $\gcd(a, b) = 1$ can be computed by the Euclidean Algorithm in time $\mathcal{O}(\log b)$. Set $r_0 = a$ and $r_1 = b$. For $i \geq 0$, divide r_i by r_{i+1}:

$$r_i = a_i r_{i+1} + r_{i+2}, \quad 0 \leq r_{i+2} < r_{i+1}.$$

This process stops when $r_{m+2} = 0$ for some $m \geq 0$.
In 1990, Wiener (Wiener, 1990) proposed an attack on RSA with modulus N and small private exponent d. The attack is based on the convergents of the continued fraction expansion of $\frac{e}{N}$.

Definition 3.2 (Convergent)**.** For $0 \leq n \leq m$, the nth convergent of the continued fraction $[a_0, a_1, \cdots, a_m]$ is $[a_0, a_1, \cdots, a_n]$.

For each $n \geq 0$, we define

$$\begin{aligned} p_{-2} &= 0, \quad p_{-1} = 1, \quad p_n = a_n p_{n-1} + p_{n-2}, \\ q_{-2} &= 1, \quad q_{-1} = 0, \quad q_n = a_n q_{n-1} + q_{n-2}. \end{aligned}$$

It is well known that the nth convergent of the continued fraction satisfies $[a_0, a_1, \cdots, a_n] = \frac{p_n}{q_n}$. More generally, there are various results satisfied by the convergents of a continued fraction. We need only the following result on Diophantine approximations (for more general information see (Hardy & Wright, 1965) and (Cohen, 1993)).

Theorem 3.1. *Let x be a real positive number. If a and b are positive integers such that* $\gcd(a, b) = 1$ *and*

$$\left| x - \frac{a}{b} \right| < \frac{1}{2b^2},$$

then $\frac{a}{b}$ is one of the convergents of the continued fraction expansion of x.

3.2 Diophantine approximations cryptanalysis of RSA

3.2.1 Wiener's attack on RSA

A well-known attack on RSA with low secret-exponent d was given by Wiener (Wiener, 1990) in 1990. Wiener showed that using continued fractions, one can efficiently recover the secret exponent d from the public key (N, e) as long as $d < \frac{1}{3}N^{\frac{1}{4}}$. For $N = pq$ with $q < p < 2q$, we present below Wiener's attack on RSA which works for the bound $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$ which is slightly better than Wiener's bound since $\frac{\sqrt{6\sqrt{2}}}{6} \geq \frac{1}{3} + 0.15$.
We will use the following useful simple lemma.

Lemma 3.2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then*

$$\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N} \quad \textit{and} \quad 2\sqrt{N} < p + q < \frac{3\sqrt{2}}{2}\sqrt{N}.$$

Proof. Suppose $q < p < 2q$. Multiplying by q, we get $q^2 < N < 2q^2$. Hence $\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N}$. Using $p = \frac{N}{q}$, we get $\sqrt{N} < p < \sqrt{2}\sqrt{N}$. This proves the first assertion. To prove the second one, observe that $(p+q)^2 = (p-q)^2 + 4N > 4N$, which gives $p + q > 2\sqrt{N}$. On the other hand, we have

$$(p+q)^2 = (p-q)^2 + 4N < \left(\sqrt{2}\sqrt{N} - \frac{\sqrt{2}}{2}\sqrt{N}\right)^2 + 4N = \frac{9}{2}N.$$

Hence $p + q < \frac{3\sqrt{2}}{2}\sqrt{N}$. This terminates the proof. □

Theorem 3.3 (Wiener)**.** *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e < \phi(N)$ a be public exponent and d be the corresponding private key. If $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$, then, we can find the factorization of N in time polynomial in* $\log N$.

Proof. We rewrite the equation $ed - k(N + 1 - p - q) = 1$ as $ed - kN = 1 - k\left(p + q - 1\right)$. Dividing by Nd, we get

$$\left|\frac{e}{N} - \frac{k}{d}\right| = \frac{\left|1 - k\left(p + q - 1\right)\right|}{Nd} < \frac{k\left(p + q - 1\right)}{Nd}. \tag{1}$$

Since $e < \phi(N)$, then $k = \frac{ed-1}{\phi(N)} < \frac{ed}{\phi(N)} < d$. Hence (1) gives

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{p + q - 1}{N} < \frac{p + q}{N}.$$

Using Lemma 3.2, this implies

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{\frac{3\sqrt{2}}{2}N^{\frac{1}{2}}}{N} = \frac{3\sqrt{2}}{2}N^{-\frac{1}{2}}.$$

Suppose that $d < \frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$, then

$$\frac{3\sqrt{2}}{2}N^{-\frac{1}{2}} < \frac{1}{2d^2},$$

and consequently

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

Hence Theorem 3.1 gives $\frac{k}{d}$ as a convergent of the continued fraction expansion of $\frac{e}{N}$. Since the continued fraction algorithm is polynomial time in $\log N$, this terminates the proof. □

3.2.2 de Weger's generalization of Wiener's attack

In 2002, de Weger (Weger, 2002) proposed a generalization of Wiener's attack on RSA. de Weger extended Wiener's bound $\frac{\sqrt{6\sqrt{2}}}{6}N^{\frac{1}{4}}$ to $d < \frac{N^{\frac{3}{4}}}{|p-q|}$ which is equivalent with Wiener's bound for the standard RSA, that is for $|p - q| = \mathcal{O}\left(N^{\frac{1}{2}}\right)$. We describe below the attack of de Weger.

Theorem 3.4 (de Weger). *Let $N = pq$ be an RSA modulus with $q < p < 2q$ and $p - q = N^{\beta}$. Let $e < \phi(N)$ a be public exponent and $d < N^{\delta}$ be the corresponding private key. If $\delta < \frac{3}{4} - \beta$, then, we can find the factorization of N in time polynomial in* $\log N$.

Proof. We transform the equation $ed - k(N + 1 - p - q) = 1$ to

$$ed - k\left(N + 1 - 2\sqrt{N}\right) = 1 - k\left(p + q - 2\sqrt{N}\right).$$

Dividing by $\left(N + 1 - 2\sqrt{N}\right)d$ and using $p + q > 2\sqrt{N}$ as proved in Lemma 3.2, we get

$$\left|\frac{e}{N + 1 - 2\sqrt{N}} - \frac{k}{d}\right| = \frac{\left|1 - k\left(p + q - 2\sqrt{N}\right)\right|}{\left(N + 1 - 2\sqrt{N}\right)d} < \frac{k\left(p + q - 2\sqrt{N}\right)}{\left(N + 1 - 2\sqrt{N}\right)d}. \tag{2}$$

Consider the terms of the right side of (2). We have $N+1-2\sqrt{N} > \frac{1}{2}N$ for $N \geq 12$. Using Lemma 3.2, we get

$$p+q-2\sqrt{N} = \frac{(p+q)^2-4N}{p+q+2\sqrt{N}} < \frac{(p-q)^2}{4\sqrt{N}}.$$

Since $e < \phi(N)$, then $k = \frac{ed-1}{\phi(N)} < \frac{ed}{\phi(N)} < d$. Consequently, the inequality (2) gives

$$\left|\frac{e}{N+1-2\sqrt{N}} - \frac{k}{d}\right| < \frac{k}{d} \cdot \frac{\frac{(p-q)^2}{4\sqrt{N}}}{\frac{1}{2}N} < \frac{(p-q)^2}{2N\sqrt{N}}.$$

In order to apply Theorem 3.1, a sufficient condition is

$$\frac{(p-q)^2}{2N\sqrt{N}} < \frac{1}{2d^2},$$

or equivalently $d < \frac{N^{\frac{3}{4}}}{|p-q|}$. Using $d < N^{\delta}$ and $|p-q| = N^{\beta}$, the condition is fulfilled if $\delta < \frac{3}{4} - \beta$. Hence we can use the continued fraction expansion of $\frac{e}{N+1-2\sqrt{N}}$ to find $\frac{k}{d}$ among the convergents. This proves the theorem. □

3.2.3 Another generalization of Wiener's attack

Let $N = pq$ be an RSA modulus with $q < p < 2q$. We present in this section an attack on RSA with a public exponent e satisfying an equation $ex - (N+1-ap-bq)y = 1$ where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$. Notice that when $a = b = 1$, the equation reduces to $ed - k(N+1-p-q) = 1$ which is the main RSA key equation. We first define the notion of approximation.

Definition 3.3. Let $N = pq$ be an RSA modulus with $q < p < 2q$ and a and b be positive integers. We say that $\frac{a}{b}$ is an approximation of $\frac{q}{p}$ if $a = \left[\frac{bq}{p}\right]$ where $[x]$ is the closest integer to the real number x.

A key role in the attack is played by the following lemma.

Lemma 3.5. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $\frac{a}{b}$ be an unknown approximation of $\frac{q}{p}$ where a is not a multiple of q. Suppose we know the integer $ap + bq$. Then we can find the factorization of N.*

Proof. Suppose we know $S = ap + bq$ where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$. We have

$$S^2 = (ap+bq)^2 = (ap-bq)^2 + 4abN. \tag{3}$$

Since, by definition, $a = \left[\frac{bq}{p}\right]$, then $\left|a - \frac{bq}{p}\right| \leq \frac{1}{2}$. Combining with Lemma 3.2, we get

$$|ap-bq| \leq \frac{1}{2}p < \frac{\sqrt{2}}{2}\sqrt{N}.$$

It follows that $(ap-bq)^2 < \frac{1}{2}N$. Hence, from (3) we derive

$$0 < \frac{S^2}{4N} - ab = \frac{(ap-bq)^2}{4N} < \frac{1}{8}.$$

This implies that ab is the integer part of $\frac{S^2}{4N}$, that is $ab = \left\lfloor \frac{S^2}{4N} \right\rfloor$. Then (3) gives

$$|ap - bq| = \sqrt{S^2 - 4\left\lfloor \frac{S^2}{4N} \right\rfloor N}.$$

Combining with $ap + bq = S$, we get

$$ap = \begin{cases} \frac{1}{2}\left(S + \sqrt{S^2 - 4\left\lfloor \frac{S^2}{4N} \right\rfloor N}\right) & \text{if} \quad ap - bq > 0, \\ \frac{1}{2}\left(S - \sqrt{S^2 - 4\left\lfloor \frac{S^2}{4N} \right\rfloor N}\right) & \text{if} \quad ap - bq < 0. \end{cases}$$

Since a is not a multiple of q, we then obtain p by computing $\gcd(ap, N)$. □

Theorem 3.6. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $\frac{a}{b}$ be an unknown approximation of $\frac{q}{p}$ and e be a public exponent satisfying an equation $ex - (N + 1 - ap - bq)y = 1$ with*

$$xy < \frac{N}{2(ap + bq)}.$$

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

Proof. Rewrite the equation $ex - (N + 1 - ap - bq)y = 1$ as $ex - Ny = 1 - (ap + bq - 1)y$ and divide by Nx. We get

$$\left|\frac{e}{N} - \frac{y}{x}\right| = \frac{|1 - (ap + bq - 1)y|}{Nx} < \frac{(ap + bq - 1)y}{Nx} < \frac{(ap + bq)y}{Nx}.$$

Suppose $xy < \frac{N}{2(ap+bq)}$, then $\frac{(ap+bq)y}{Nx} < \frac{1}{2x^2}$. Hence, by Theorem 3.1, $\frac{y}{x}$ is a convergent of the continued fraction expansion of $\frac{e}{N}$. Since $\gcd(x, y) = 1$, this gives x and y. Next, we use x and y to transform the equation $ex - (N + 1 - ap - bq)y = 1$ to $ap + bq = N + 1 - \frac{ex-1}{y}$, where the right hand side is completely known. Hence, using Lemma 3.5, we find the factorization of N in polynomial time. □

In Section 4.3.4, we will present an attack on RSA when the public exponent e satisfies the same equation $ex - (N + 1 - ap - bq)y = 1$ using lattice reduction methods.

3.2.4 Nassr et al. generalization of Wiener's attack

Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose we know an approximation p_0 of p with $|p - p_0| < \frac{1}{8}N^{\alpha}$. In 2008, Nassr et al. (Nassr et al., 2008) presented a continued fraction attack on RSA with a private exponent satisfying $d < N^{\frac{1-\alpha}{2}}$.

Theorem 3.7. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Suppose we know an approximation p_0 of p with $|p - p_0| < \frac{1}{8}N^{\alpha}$. Let e be a public exponent. If the corresponding private exponent d satisfies $d < N^{\frac{1-\alpha}{2}}$, then N can be factored in time polynomial in* $\log N$.

Proof. Set $c = \frac{1}{8}$. Suppose we know $p_0 > \sqrt{N}$ and α such that $|p - p_0| < cN^\alpha$. Then $p_0 - cN^\alpha < p < p_0 + cN^\alpha$. By lemma 3.2, we should also suppose $\sqrt{N} < p_0 - cN^\alpha$ and $p_0 + cN^\alpha < \sqrt{2}\sqrt{N}$. Using $q = \frac{N}{p}$, we get

$$\frac{N}{p_0 + cN^\alpha} < q < \frac{N}{p_0 - cN^\alpha}.$$

It follows that

$$p_0 + \frac{N}{p_0 + cN^\alpha} - cN^\alpha < p + q < p_0 + \frac{N}{p_0 - cN^\alpha} + cN^\alpha.$$

Define P as the mean value

$$P = \frac{1}{2}\left(2p_0 + \frac{N}{p_0 + cN^\alpha} + \frac{N}{p_0 - cN^\alpha}\right) = p_0 + \frac{Np_0}{p_0^2 - c^2N^{2\alpha}}.$$

Then

$$|p + q - P| < \frac{1}{2}\left(\frac{N}{p_0 - cN^\alpha} - \frac{N}{p_0 + cN^\alpha} + 2cN^\alpha\right) = \frac{cN^{1+\alpha}}{p_0^2 - c^2N^{2\alpha}} + cN^\alpha.$$

Since $p_0 - cN^\alpha > \sqrt{N}$, then $p_0 + cN^\alpha > \sqrt{N}$ and $p_0^2 - c^2N^{2\alpha} > N$. Hence

$$|p + q - P| < \frac{cN^{1+\alpha}}{p_0^2 - cN^{2\alpha}} + cN^\alpha < \frac{cN^{1+\alpha}}{N} + cN^\alpha = 2cN^\alpha.$$

Rewrite the key equation $ed - k\phi(N) = 1$ as $ed - k(N + 1 - P) = 1 + k(P - p - q)$. We divide by $(N + 1 - P)d$ and get

$$\left|\frac{e}{N + 1 - P} - \frac{k}{d}\right| = \frac{|1 + k(P - p - q)|}{(N + 1 - P)d} < \frac{1 + k|P - p - q|}{(N + 1 - P)d} \leq \frac{(1 + k)|P - p - q|}{(N + 1 - P)d}.$$

Since $k = \frac{ed-1}{\phi(N)} < d$, then $1 + k \leq d$. Combining this with $|p + q - P| < 2cN^\alpha$, we get

$$\left|\frac{e}{N + 1 - P} - \frac{k}{d}\right| < \frac{2cN^\alpha}{N + 1 - P}.$$

By Lemma 3.2, we have $P < \frac{3\sqrt{2}}{2}\sqrt{N}$. Then, for $N \geq 14$, we get

$$N + 1 - P > N + 1 - \frac{3\sqrt{2}}{2}\sqrt{N} > \frac{1}{2}N.$$

This implies that $\left|\frac{e}{N+1-P} - \frac{k}{d}\right| < 4cN^{\alpha-1}$. In order to apply Theorem 3.1, we must have $4cN^{\alpha-1} < \frac{1}{2d^2}$. This is fulfilled if

$$d < \frac{1}{\sqrt{8c}}N^{\frac{1-\alpha}{2}} = N^{\frac{1-\alpha}{2}},$$

where we used $c = \frac{1}{8}$. Using $d = N^\delta$, a sufficient condition is $\delta < \frac{1-\alpha}{2}$. Then $\frac{k}{d}$ is a convergent of $\frac{e}{N+1-P}$. Using k and d, we get the factorization of N in polynomial time. □

Notice that when $\alpha = \frac{1}{2}$, the bound is $d < N^{\frac{1}{4}}$ as expected in Wiener's attack (Theorem 3.3).

4. Lattices

4.1 Background on lattices

The most powerful attacks on RSA are based on techniques that use lattice basis reduction algorithms, such as the LLL algorithm. Invented by Lenstra, Lenstra and Lovász (Lenstra et al., 1982) in 1982, LLL is a polynomial time algorithm for lattice basis reduction with many applications in cryptography. A typical example of the powers of the LLL algorithm is the following problem.

Small roots of a modular polynomial problem: Given a composite N with unknown factorization and a polynomial $f(x)$ of degree d, find all small solutions x_0 to the polynomial equation $f(x) \equiv 0 \pmod{N}$.

In his seminal work, Coppersmith (Coppersmith, 1997) solved this problem in 1996 for solutions x_0 satisfying $|x_0| < N^{\frac{1}{d}}$ using the LLL algorithm.
In this section, we give the mathematical background on lattices and the LLL algorithm for basis reduction. We start by giving a formal definition of a lattice.

Definition 4.1 (Lattice)**.** Let $n \leq m$ be two positive integers and $b_1, \cdots, b_n \in \mathbb{R}^m$ be n linearly independent vectors. A lattice $\mathcal{L}$ spanned by $\{b_1, \cdots, b_n\}$ is the set of all integer linear combinations of $b_1, \cdots, b_n$, that is

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} x_i b_i \mid x_i \in \mathbb{Z} \right\}.$$

The set $\langle b_1 \ldots, b_n \rangle$ is called a lattice basis for $\mathcal{L}$. The lattice dimension is $\dim(\mathcal{L}) = n$.

In general, a basis for $\mathcal{L}$ is any set of independent vectors that generates $\mathcal{L}$. Any two bases for a lattice $\mathcal{L}$ are related by a matrix having integer coefficients and determinant equal to ± 1. Hence, all the bases have the same Gramian determinant $\det_{1\leq i,j\leq n} \left\langle b_i, b_j \right\rangle$ where $\left\langle b_i, b_j \right\rangle$ denotes the scalar product of vectors b_i, b_j. The determinant of the lattice is then

$$\det(\mathcal{L}) = \left(\det_{1\leq i,j\leq n} \left\langle b_i, b_j \right\rangle \right)^{\frac{1}{2}}.$$

Let $v = \sum_{i=1}^{n} x_i b_i$ be a vector of $\mathcal{L}$. We define the Euclidean norm of v as

$$\|v\| = \left(\sum_{i=1}^{n} x_i^2 \right)^{\frac{1}{2}}.$$

Given a basis $\langle b_1 \ldots, b_n \rangle$ of the lattice $\mathcal{L}$, the Gram-Schmidt process gives an orthogonal set $\langle b_1^* \ldots, b_n^* \rangle$. The determinant of the lattice is then $\det(\mathcal{L}) = \prod_{i=1}^{n} \|b_i^*\|$. The Gram-Schmidt procedure starts with $b_1^* = b_1$, and then for $i \geq 2$,

$$i \geq 2, \quad b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*, \quad \text{where} \quad \mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \quad \text{for} \quad 1 \leq j < i.$$

Note that $\langle b_1^* \ldots, b_n^* \rangle$ is not a basis of the lattice $\mathcal{L}$. Since every nontrivial lattice has infinitely many bases, some bases are better than others. The most important quality measure is the length of the basis vectors. For arbitrary lattices, the problem of computing a shortest vector is known to be NP-hard under randomized reductions (Ajtai, 1998). However, in many applications, the LLL algorithm computes in polynomial time a reduced basis with nice properties.

Definition 4.2 (LLL Reduction)**.** Let $B = \langle b_1, \ldots, b_n \rangle$ be a basis for a lattice $\mathcal{L}$ and let $B^* = \langle b_1^*, \ldots, b_n^* \rangle$ be the associated Gram-Schmidt orthogonal basis. Let

$$\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \quad \text{for} \quad 1 \leq j < i.$$

The basis B is said to be LLL reduced if it satisfies the following two conditions:

$$|\mu_{i,j}| \leq \frac{1}{2}, \quad \text{for} \quad 1 \leq j < i \leq n,$$
$$\frac{3}{4}\|b_{i-1}^*\|^2 \leq \|b_i^* + \mu_{i,i-1} b_{i-1}^*\|^2 \quad \text{for} \quad 1 < i \leq n.$$

Below we give useful inequalities satisfied by an LLL reduced basis derived from the LLL reduction definition (for a proof see e.g. (Cohen, 1993; Lenstra et al., 1982; May, 2003)).

Theorem 4.1. *Let $\mathcal{L}$ be a lattice of dimension n. Let $B = \langle b_1, \ldots, b_n \rangle$ be an LLL reduced basis and let $B^* = \{b_1^*, \ldots, b_n^*\}$ be the associated Gram-Schmidt orthogonal basis. Then*

$$\|b_1\| \leq \|b_2\| \leq \ldots \leq \|b_i\| \leq 2^{\frac{n(n-i)}{4(n+1-i)}} (\det(\mathcal{L}))^{\frac{1}{n+i-1}} \quad \textit{for} \quad 1 \leq i \leq n.$$

4.2 Small solution of polynomial equations

In this section, we present some applications of lattices in finding small roots to polynomial equations. We provide some very useful theorems that will make the analysis of RSA much easier to follow. This includes the seminal work of Coppersmith (Coppersmith, 1997) for finding small roots of univariate modular polynomial equations, the recently proposed method of Herrmann and May (Herrmann & May, 2008) for solving the bivariate linear modular equation, and the small inverse problem introduced by Boneh and Durfee in (Boneh & Durfee, 1999). The main idea behind these methods is to transform a modular polynomial equation to an equation over the integers. We need the following definition.

Definition 4.3. Given a polynomial $f(x_1, \ldots, x_n) = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} x^{i_1} \cdots x^{i_n}$ and real positive numbers $X_1, \ldots, X_n$, we define the Euclidean norm of $f(X_1 x_1, \ldots, X_n x_n)$ by

$$\|f(X_1 x_1, \ldots, X_n x_n)\| = \left(\sum_{i_1,\ldots,i_n} \left(a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n} \right)^2 \right)^{\frac{1}{2}}.$$

4.2.1 Howgrave-Graham's theorem

To transform a modular polynomial equation $h(x_1, \ldots, x_n) \equiv 0 \pmod{B}$ into a polynomial equation $h(x_1, \ldots, x_n) = 0$ over the integers, a sufficient condition is given by the following theorem by Howgrave-Graham (Howgrave-Graham, 1997) who reformulated Coppersmith's ideas of finding modular roots.

Theorem 4.2 (Howgrave-Graham). *Let $h(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial with at most ω monomials. Suppose that $h(x_1^{(0)}, \ldots, x_n^{(0)}) \equiv 0 \pmod{B}$ where $|x_0^{(0)}| < X_1, \ldots, |x_n^{(0)}| < X_n$ and $\|h(X_1 x_1, \ldots, X_n x_n)\| < \frac{B}{\sqrt{\omega}}$. Then $h(x_1^{(0)}, \ldots, x_n^{(0)}) = 0$ holds over the integers.*

Proof. Let $h(x_1, \ldots, x_n) = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n}$ with ω monomials. We have

$$\left|h(x_1^{(0)}, \ldots, x_n^{(0)})\right| = \left|\sum a_{i_1,\ldots,i_n} \left(x_1^{(0)}\right)^{i_1} \ldots \left(x_n^{(0)}\right)^{i_n}\right| \leq \sum \left|a_{i_1,\ldots,i_n} \left(x_1^{(0)}\right)^{i_1} \ldots \left(x_n^{(0)}\right)^{i_n}\right|.$$

Suppose $|x_0^{(0)}| < X_1, \ldots, |x_n^{(0)}| < X_n$. Then

$$\left|h(x_1^{(0)}, \ldots, x_n^{(0)})\right| < \sum \left|a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}\right|. \tag{4}$$

For $(a, b) \in \mathbb{R}^2$, the Cauchy-Schwarz inequality states that

$$\left(\sum_k a_k b_k\right)^2 \leq \sum_k a_k^2 \sum_k b_k^2.$$

Using this with $a_k = 1$ and $b_k = a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$, we get

$$\left(\sum \left|a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}\right|\right)^2 \leq \sum 1^2 \sum \left(a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}\right)^2 = \omega \|h(X_1 x_1, \ldots, X_n x_n)\|^2,$$

which gives

$$\sum \left|a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}\right| \leq \sqrt{\omega} \|h(X_1 x_1, \ldots, X_n x_n)\|. \tag{5}$$

Now, suppose that $\|h(X_1 x_1, \ldots, X_n x_n)\| < \frac{B}{\sqrt{\omega}}$. Then combining (4) and (5), we get

$$\left|h(x_1^{(0)}, \ldots, x_n^{(0)})\right| < \sum \left|a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}\right| < \sqrt{\omega} \|h(X_1 x_1, \ldots, X_n x_n)\| < B.$$

Hence if $h(x_1^{(0)}, \ldots, x_n^{(0)}) \equiv 0 \pmod{B}$, then $h(x_1^{(0)}, \ldots, x_n^{(0)}) = 0$ holds over the integers. □

4.2.2 Coppersmith's theorem

In 1996, Coppersmith (Coppersmith, 1997) described very clever techniques to find small modular roots of univariate polynomials and small integer roots of bivariate polynomials. The idea behind Coppersmith's method for finding a small root of a polynomial f is to reduce this problem to finding the same small root of a polynomial h over the integers. We present a generalization of Coppersmith's result for univariate modular polynomial equations as given by May (May, 2003) in 2003.

Theorem 4.3. *Let N be an integer of unknown factorization, which has a divisor $b > N^\beta$. Let $f_b(x)$ be a monic univariate polynomial of degree d and $\varepsilon > 0$. Then we can find all solutions x_0 for the equation $f_b(x) \equiv 0 \pmod{b}$ such that $|x_0| < \frac{1}{2} N^{\frac{\beta^2}{d} - \varepsilon}$ in polynomial time.*

Proof. We fix two integers m, t and define a set of univariate polynomials $g_{i,j}(x)$ by

$$g_{i,j}(x) = x^i (f_b(x))^j N^{m-j}, \quad j = 0, \ldots, m, \quad 0 \leq i \leq t - 1.$$

Since $f_b(x_0) \equiv 0 \pmod{b}$, then $(f_b(x_0))^j N^{m-j} \equiv 0 \pmod{b^m}$. This means that all polynomials $g_{i,j}(x)$ share the root x_0 modulo N^m. Hence, any integer linear combination $h(x)$ of the polynomials $g_{i,j}(x)$ also has the root x_0 modulo N^m. The goal is to find a polynomial $h(x)$

satisfying the conditions of Howgrave-Graham's Theorem 4.2 and then solve $h(x)$ over the integers. Notice that the degrees of the polynomials $g_{i,j}(Xx)$ satisfy

$$0 \leq \deg_{i,j} g_{i,j}(Xx) \leq dm + t - 1.$$

Let $n \geq (m+1)d - 1$. We consider the lattice $\mathcal{L}$ generated by a basis matrix whose rows are the coefficient vectors of $g_{i,j}(Xx)$ for $j = 0, \ldots, m$ and $0 \leq i \leq d-1$, completed with the polynomials $r_k = x^k$ for $(m+1)d \leq k \leq n-1$. We get a triangular matrix as illustrated in Fig. 1 where I_k is the unit matrix of size $(n - (m+1)d + 1) \times (n - (m+1)d + 1)$.

$$\begin{array}{c||cccc|c|ccc|c|ccc||c}
 & 1 & x & \ldots & x^{d-1} & \ldots & x^{dj} & \ldots & x^{(j+1)d-1} & \ldots & x^{dm} & \ldots & x^{(m+1)d-1} & \ldots x^{n-1} \\
\hline\hline
g_{0,0} & N^m & & & & & & & & & & & & \\
g_{1,0} & & N^m X & & & & & & & & & & & \\
\vdots & & & \ddots & & & & & & & & & & \\
g_{d-1,0} & & & & N^m X^{d-1} & & & & & & & & & \\
\hline
\vdots & * & * & \ldots & * & \ddots & & & & & & & & \\
\hline
g_{0,j} & * & * & \ldots & * & \ldots & N^{m-j}X^{dj} & & & & & & & \\
\vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \ldots & \ddots & & & & & & \\
g_{d-1,j} & * & * & \ldots & * & \ldots & * & \ldots & N^{m-j}X^{(d+1)j-1} & & & & & \\
\hline
\vdots & * & * & \ldots & * & \ldots & * & \ldots & * & \ddots & & & & \\
\hline
g_{0,m} & * & * & \ldots & * & \ldots & * & \ldots & * & \ldots & X^{dm} & & & \\
\vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \ldots & \ddots & & \\
g_{d-1,m} & * & * & \ldots & * & \ldots & * & \ldots & * & \vdots & * & \ldots & X^{(m+1)d-1} & \\
\hline\hline
(r_k) & & & & & & & & & & & & & I_k
\end{array}$$

Fig. 1. Coppersmith's matrix of the polynomials $g_{i,j}(Xx)$ and $r_k(x)$ in the basis $\left(1, \ldots, x^{n-1}\right)$.

The determinant of the lattice $\mathcal{L}$ is $\det(\mathcal{L}) = N^{\frac{1}{2}m(m+1)d} X^{\frac{1}{2}n(n-1)}$ where $n \geq (m+1)d - 1$ is the dimension of $\mathcal{L}$. Applying Theorem 4.1 with $i = 1$, we get an LLL-reduced basis with a small vector $h(x)$ satisfying

$$\|h(Xx)\| \leq 2^{\frac{1}{4}(n-1)} (\det(\mathcal{L}))^{\frac{1}{n}} = 2^{\frac{1}{4}(n-1)} N^{\frac{1}{2n}m(m+1)d} X^{\frac{1}{2}(n-1)}.$$

Moreover, we have $h(x_0) \equiv 0 \pmod{b}^m$. If $\|h(Xx)\| \leq \frac{b^m}{\sqrt{n}}$, then Howgrave-Graham's result 4.2 applies and we can find x_0 by solving $h(x) = 0$ over the integers. A sufficient condition is then

$$2^{\frac{1}{4}(n-1)} \cdot N^{\frac{1}{2n}m(m+1)d} \cdot X^{\frac{1}{2}(n-1)} < \frac{b^m}{\sqrt{n}},$$

which implies

$$X < 2^{-\frac{1}{2}} \cdot N^{-\frac{m(m+1)d}{n(n-1)}} \cdot b^{\frac{2m}{n-1}} n^{-\frac{1}{n-1}}.$$

Since $b \geq N^{\beta}$, this holds if

$$X < 2^{-\frac{1}{2}} \cdot n^{-\frac{1}{n-1}} \cdot N^{\frac{(2n\beta-(m+1)d)m}{n(n-1)}}.$$

Consider the term $\frac{(2n\beta-(m+1)d)m}{n(n-1)}$ as a function of m. We obtain a lower bound by substituting $m = \frac{2n\beta-d}{2d}$, namely

$$\frac{(2n\beta - (m+1)d)m}{n(n-1)} \geq \frac{\beta^2}{d} - \frac{d}{4n} + \frac{(d-2\beta)^2}{(n-1)d} \geq \frac{\beta^2}{d} - \varepsilon,$$

where $\varepsilon = \left| \frac{d}{4n} - \frac{(d-2\beta)^2}{(n-1)d} \right|$. It follows that a sufficient condition for X is that

$$X \leq 2^{-\frac{1}{2}} \cdot n^{-\frac{1}{n-1}} \cdot N^{\frac{\beta^2}{d}-\varepsilon}.$$

Since $2^{-\frac{1}{2}} n^{-\frac{1}{n-1}} > \frac{1}{2}$ for $n \geq 7$, the condition reduces to $X < \frac{1}{2}N^{\frac{\beta^2}{d}-\varepsilon}$, which concludes the proof. □

From the previous theorem, we deduce the following result where the term ε is canceled.

Theorem 4.4 (Coppersmith). *Let N be an integer of unknown factorization. Let $b \geq N^{\beta}$ be a divisor of N and $f_b(x)$ be a univariate, monic polynomial of degree d. 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 $f_b(x) \equiv 0 \pmod{b}$ such that $|x_0| < c_N N^{\frac{\beta^2}{d}}$ in time polynomial in $(\log N, d)$.*

Proof. With the parameter choice $\varepsilon = \frac{1}{\log N}$, we get

$$\frac{1}{2}N^{\frac{\beta^2}{d}-\varepsilon} = \frac{1}{2}N^{\frac{\beta^2}{d}}N^{-\varepsilon} = \frac{1}{2}N^{\frac{\beta^2}{d}}N^{-\frac{1}{\log N}} = \frac{1}{4}N^{\frac{\beta^2}{d}}$$

where we used $N^{-\frac{1}{\log N}} = \frac{1}{2}$. Hence, Theorem 4.3 implies that one can find all solutions x_0 of the equation $f_b(x) \equiv 0 \pmod{b}$ such that $|x_0| < \frac{1}{4}N^{\frac{\beta^2}{d}}$ in time polynomial in $(\log N, d)$. To find all solutions x_0 of the equation $f_b(x) \equiv 0 \pmod{b}$ such that $|x_0| < c_N N^{\frac{\beta^2}{d}}$, we consider the $4c_N$ different intervals in $\left[-c_N N^{\frac{\beta^2}{d}}, c_N N^{\frac{\beta^2}{d}}\right]$, each of size $\frac{1}{4}N^{\frac{\beta^2}{d}}$ and centered at $x_i = -c_N + \frac{2i+1}{8}$ for $i \geq 0$. In each interval, we can apply Theorem 4.3 with the polynomial $f_b(x - x_i)$ and get all solutions. □

4.2.3 Herrmann and May's theorem for bivariate modular linear equations

In 2008, Herrmann and May (Herrmann & May, 2008) proposed a method for solving the bivariate modular linear equation $f(x,y) = ax + by + c \equiv 0 \pmod{p}$ where p is an unknown divisor of N. We review below the method. The method relies on the following standard assumption in order to extract the solution (x_0, y_0) efficiently.

Assumption 1. Let $h_1(x_1,\ldots,x_n),\ldots,h_n(x_1,\ldots,x_n) \in \mathbb{Z}[x_1,\ldots,x_n]$ be the polynomials that are found by Coppersmith's algorithm. Then the ideal generated by the polynomial equations $h_1(x_1,\ldots,x_n) = 0, \cdots, h_n(x_1,\ldots,x_n) = 0$ has dimension zero. Equivalently, the resultant computations of the h_i yield nonzero polynomials.

Theorem 4.5 (Herrmann-May). *Let $\varepsilon > 0$ and let N be a sufficiently large composite integer of unknown factorization with a divisor $p > N^{\beta}$. Furthermore, let $f(x,y) \in \mathbb{Z}[x,y]$ be a linear polynomial in two variables. Then, one can find all solutions (x_0, y_0) of the equation $f(x,y) \equiv 0 \pmod{p}$ with $|x_0| < N^{\gamma}$ and $|y_0| < N^{\delta}$ if*

$$\gamma + \delta \leq 3\beta - 2 + 2(1-\beta)^{\frac{3}{2}} - \varepsilon.$$

The time complexity of the algorithm is polynomial in $\log N$ and $\frac{1}{\varepsilon}$.

Proof. Suppose $f(x,y) = ax + by + c \equiv 0 \pmod{p}$. Multiplying by $a^{-1} \pmod{N}$, we get $f(x,y) = x + b'y + c' \equiv 0 \pmod{p}$. Thus, we can assume that $f(x,y) = x + by + c$. To find a solution (x_0, y_0), the basic idea consists in finding two polynomials $h_1(x,y)$ and $h_2(x,y)$ such that $h_1(x_0,y_0) = h_1(x_0,y_0) = 0$ holds over the integers. Then the resultant of $h_1(x,y)$ and $h_2(x,y)$ will reveal the root (x_0, y_0). To do so, we generate a collection of polynomials $g_{k,i}(x,y)$ as

$$g_{k,i}(x,y) = y^i \cdot f(x,y)^k \cdot N^{\max\{t-k,0\}}$$

for $0 \leq k \leq m, 0 \leq i \leq m-k$ and integer parameters $t < m$ that will be specified later. Observe that the polynomials $g_{k,i}(x,y)$ share the common root (x_0, y_0) modulo $p^{k+\max\{t-k,0\}} \geq p^t$. The ordering for the polynomials is as follows. If $k < l$, then $g_{k,i} < g_{l,j}$. If $k = l$ and $i < j$, then $g_{k,i} < g_{k,j}$. On the other hand, each polynomial $g_{k,i}(x,y)$ is ordered in the monomials $x^i y^k$. The ordering for the monomials $x^i y^k$ is as follows. If $i < j$, then $x^i y^k < x^j y^l$. If $i = j$ and $k < l$, then $x^i y^k < x^i y^l$. Let X and Y be positive integers. Gathering the coefficients of the polynomials $g_{k,i}(Xx, Yy)$, we obtain a matrix as illustrated in Fig. 2.

$$\begin{array}{c||ccc|ccc|c|ccc|c|c}
 & 1 & \cdots & y^m & x & \cdots & xy^{m-1} & \cdots & x^t & \cdots & x^t y^{m-t} & \cdots & x^m \\
\hline\hline
g_{0,0} & N^t & & & & & & & & & & & \\
\vdots & & \ddots & & & & & & & & & & \\
g_{0,m} & & & N^t Y^m & & & & & & & & & \\
\hline
g_{1,0} & * & \cdots & * & N^{t-1}X & & & & & & & & \\
\vdots & * & \cdots & * & & \ddots & & & & & & & \\
g_{1,m-1} & * & \cdots & * & * & \cdots & N^{t-1}XY^{m-1} & & & & & & \\
\hline
\vdots & * & \vdots & * & * & \vdots & * & \ddots & & & & & \\
\hline
g_{t,0} & * & \cdots & * & * & \cdots & * & \cdots & X^t & & & & \\
\vdots & & \vdots & & & \vdots & & \vdots & & \ddots & & & \\
g_{t,m-t} & * & \cdots & * & * & \cdots & * & \cdots & * & \cdots & X^t Y^{m-t} & & \\
\hline
\vdots & * & \vdots & * & * & \vdots & * & \vdots & * & \vdots & * & \ddots & \\
\hline
g_{m,0} & * & \cdots & * & * & \cdots & * & \cdots & * & \cdots & * & \cdots & X^m
\end{array}$$

Fig. 2. Herrmann-May's matrix of the polynomials $g_{k,i}(Xx, Yy)$ in the basis $\langle x^r y^s \rangle_{0 \leq r \leq m, 0 \leq s \leq m-r}$.

Let $\mathcal{L}$ be the lattice of row vectors from the coefficients of the polynomials $g_{k,i}(Xx, Yy)$ in the basis $\langle x^k y^i \rangle_{0 \leq k \leq m, 0 \leq i \leq m-r}$. The dimension of $\mathcal{L}$ is

$$n = \sum_{i=0}^{m} (m+1-i) = \frac{(m+2)(m+1)}{2}.$$

From the triangular matrix of the lattice, we can easily compute the determinant $\det(\mathcal{L}) = X^{s_x}Y^{s_y}N^{s_N}$ where

$$s_x = \sum_{i=0}^{m} i(m+1-i) = \frac{m(m+1)(m+2)}{6},$$
$$s_y = \sum_{i=0}^{m}\sum_{j=0}^{m-i} j = \frac{m(m+1)(m+2)}{6},$$
$$s_N = \sum_{i=0}^{t}(t-i)(m+1-i) = \frac{t(t+1)(3m+4-t)}{6}.$$

We want to find two polynomials with short coefficients that contain all small roots over the integer. Applying Theorem 4.1 with $i = 2$, we find two polynomials $h_1(x, y)$ and $h_2(x, y)$ such that

$$\|h_1(Xx, Yy)\| \leq \|h_2(Xx, Yy)\| \leq 2^{n/4}(\det(\mathcal{L}))^{1/(n-1)}.$$

To apply Howgrave-Graham's Theorem 4.2 for $h_1(Xx, Yy)$ and $h_2(Xx, Yy)$ with $B = p^t$, a sufficient condition is that

$$2^{n/4}(\det(\mathcal{L}))^{1/(n-1)} \leq \frac{p^t}{\sqrt{n}}.$$

Put $X = N^{\gamma}$ and $Y = N^{\delta}$. We have $n = \frac{(m+2)(m+1)}{2}$ and $\det(\mathcal{L}) = X^{s_x}Y^{s_y}N^{s_N} = N^{s_x(\gamma+\delta)+s_N}$. Then the condition transforms to

$$2^{\frac{(m+2)(m+1)}{8}} N^{\frac{2(\gamma+\delta)s_x+2s_N}{m(m+3)}} \leq \frac{N^{\beta t}}{\sqrt{\frac{(m+2)(m+1)}{2}}}.$$

Define $\varepsilon_1 > 0$ such that

$$\frac{2^{-\frac{(m+2)(m+1)}{8}}}{\sqrt{\frac{(m+2)(m+1)}{2}}} = N^{-\varepsilon_1}.$$

Then, the condition simplifies to

$$\frac{2(\gamma+\delta)s_x + 2s_N}{m(m+3)} \leq \beta t - \varepsilon_1.$$

Neglecting the ε_1 term and using $s_x = \frac{m(m+1)(m+2)}{6}$ and $s_N = \frac{t(t+1)(3m+4-t)}{6}$, we get

$$\frac{m(m+1)(m+2)}{3}(\gamma+\delta) + \frac{t(t+1)(3m+4-t)}{3} < m(m+3)\beta t.$$

Define $0 < \tau < 1$ by $t = \tau m$. Then, the condition becomes

$$(m+1)(m+2)(\gamma+\delta) + \tau(m\tau+1)(3m+4-m\tau) < 3m(m+3)\beta\tau,$$

which leads to

$$\begin{aligned}\gamma+\delta &< \frac{3m(m+3)\beta\tau - \tau(m\tau+1)(3m+4-m\tau)}{(m+1)(m+2)}\\ &= \left(\tau^2 - 3\tau + 3\beta\right)\tau + \frac{\left(\tau^2-1-6\beta\right)\tau}{m+1} - \frac{2\left(2\tau^2-3\tau-3\beta+1\right)\tau}{m+2}.\end{aligned}$$

The term $\left(3\beta+\tau^2-3\tau\right)\tau$ is optimal for the value $\tau = 1-\sqrt{1-\beta}$. Hence, the bound reduces to

$$\gamma+\delta < 3\beta-2+2(1-\beta)^{\frac{3}{2}}+\frac{3-9\beta+(7\beta-3)\sqrt{1-\beta}}{m+1}+\frac{12\beta-6+(6-10\beta)\sqrt{1-\beta}}{m+2}.$$

Now, consider the last two fractions. We have

$$\frac{3-9\beta+(7\beta-3)\sqrt{1-\beta}}{m+1}+\frac{12\beta-6+(6-10\beta)\sqrt{1-\beta}}{m+2}\approx-\frac{3(1-\beta)\left(1-\sqrt{1-\beta}\right)}{m+1}.$$

Hence $\gamma+\delta < 3\beta-2+2(1-\beta)^{\frac{3}{2}}-\varepsilon$, where $\varepsilon \geq \frac{3(1-\beta)\left(1-\sqrt{1-\beta}\right)}{m+1} > 0$. Observe that this leads to $m \geq \frac{3(1-\beta)\left(1-\sqrt{1-\beta}\right)}{\varepsilon}-1$. The algorithm's complexity depends mainly on the complexity of the LLL algorithm which is polynomial in the lattice dimension and the lattice coefficients. Recall that the dimension of our lattice is $n = \frac{(m+2)(m+1)}{2} = \mathcal{O}\left(m^2\right)$ and that the lattice coefficients are bounded by $Y^m N^t \leq N^{m+\tau m}$ and have bitsize $\mathcal{O}(m\log(N))$. Consequently, the running time of the method is polynomial in $\log(N)$ and $1/\varepsilon$. □

4.2.4 The small inverse problem

In 1999, Boneh and Durfee introduced the so called small inverse problem. Let A, B, X and Y be fixed positive integers. The problem is to find all solutions (x_0, y_0) for the equation $x(A+y) \equiv 1 \pmod{B}$, with $|x_0| < X$ and $|y_0| < Y$. The method makes use of Coppersmith's technique and is generalized in the following theorem.

Theorem 4.6. *Let B be a positive integer. Consider the polynomial $f(x,y) = a_0 + a_1 x + xy$. Let $X = B^\delta$, $Y = B^\beta$. If $f(x,y) \equiv 0 \pmod{B}$ with $|x_0| < X$ and $|y_0| < Y$ and*

$$\delta < 1+\frac{1}{3}\beta-\frac{2}{3}\sqrt{\beta^2+3\beta},$$

then we can we find two polynomials h_1, h_2 such that $h_1(x_0,y_0) = h_2(x_0,y_0) = 0$ and, under Assumption1, we can extract x_0, y_0 in time polynomial in $\log N$.

Proof. We use the extended strategy of Jochemsz and May (Jochemsz & May, 2006) for finding small modular roots. Let m and t be given positive integers. For $0 \leq k \leq m$, define the set

$$M_k = \bigcup_{0\leq j\leq t}\left\{x^{i_1}y^{i_2+j} \;\middle|\; x^{i_1}y^{i_2} \quad \text{monomial of} \quad f^m \quad \text{and} \quad \frac{x^{i_1}y^{i_2}}{(xy)^k} \quad \text{monomial of} \quad f^{m-k}\right\}.$$

Hence, for $0 \leq k \leq m$, we obtain

$$x^{i_1}y^{i_2} \in M_k \text{ for } i_1 = k,\ldots,m \quad \text{and} \quad i_2 = k,\ldots,i_1+t.$$

For $0 \leq k \leq m$, define the polynomials

$$g_{i_1,i_2,k}(x,y) = \frac{x^{i_1}y^{i_2}}{(xy)^k}f(x,y)^k B^{m-k} \quad \text{with} \quad x^{i_1}y^{i_2} \in M_k \backslash M_{k+1}.$$

For $0 \leq k \leq m$, these polynomials reduce to

$$g_{i_1,k,k}(x,y) = x^{i_1-k}f(x,y)^k B^{m-k}, \quad k \leq i_1 \leq m,$$
$$g_{k,i_2,k}(x,y) = y^{i_2-k}f(x,y)^k B^{m-k}, \quad k+1 \leq i_2 \leq k+t,.$$

For each tuple (i_1, i_2, k), we have $g_{i_1,i_2,k}(x_0, y_0) \equiv 0 \pmod{B^m}$. Hence, we can search for a small norm integer linear combination of the polynomials $g_{i_i,i_2,k}(Xx, Yy)$ and apply Howgrave's theorem 4.2. These polynomials are found using lattice basis reduction. Consider the lattice $\mathcal{L}$ generated by the basis matrix whose rows are the coefficient vectors of $g_{i_1,i_2,k}(Xx, Yy)$ in the basis $\left(x^{i_1}y^{i_2}\right)$. The ordering of the monomials is as follows. If $i_2 < i_2'$, then $x^{i_1}y^{i_2} < x^{i_1'}y^{i_2'}$. If $i_2 = i_2'$ and $i_1 < i_1'$, then $x^{i_1}y^{i_2} < x^{i_1'}y^{i_2'}$. We obtain a triangular matrix M of the form

$$M(\mathcal{L}) = \begin{bmatrix} M_0 & & & & \\ * & \ddots & & & \\ * & * & M_k & & \\ \vdots & \vdots & \vdots & \ddots & \\ * & * & * & * & M_m \end{bmatrix},$$

where M_k is a triangular square matrix corresponding to the polynomials $g_{i_1,k,k}(Xx, Yy)$ and $g_{k,i_2,k}(Xx, Yy)$ as given in Fig. 3.

	$x^k y^k$	$x^{k+1} y^k$	$\ldots$	$x^m y^k$	$x^k y^{k+1}$	$\ldots$	$x^k y^{k+t}$
$g_{k,k,k}$	$B^{m-k}X^kY^k$						
$g_{k+1,k,k}$		$B^{m-k}X^{k+1}Y^k$					
$\vdots$			$\ddots$				
$g_{m,k,k}$				$B^{m-k}X^mY^k$			
$g_{k,k+1,k}$					$B^{m-k}X^kY^{k+1}$		
$\vdots$						$\ddots$	
$g_{k,k+t,k}$							$B^{m-k}X^kY^{k+t}$

Fig. 3. Diagonal part of the matrix of the polynomials $g_{i_1,k,k}(Xx, Yy)$, $k \leq i_1 \leq m$ and $g_{k,i_2,k}(Xx, Yy)$, $k + 1 \leq i_2 \leq k + t$.

For $0 \leq m$, we have $\text{rank}(M_k) = m - k + 1 + t$ and $\det(M_k) = B^s_{B,k} X^s_{x,k} Y^s_{y,k}$ where

$$s_{B,k} = (m-k)\text{rank}(M_k) = (m-k)(m-k+1+t).$$

$$s_{x,k} = tk + \sum_{i=k}^{m} i = tk + \frac{(m+k)(m+1-k)}{2}.$$

$$s_{y,k} = (m-k+1)k + \sum_{i=k+1}^{k+t} i = (m-k+1)k + \frac{(t+2k+1)t}{2}.$$

Hence, the dimension of the lattice $\mathcal{L}$ is

$$n = \dim(\mathcal{L}) = \sum_{k=0}^{m} \text{rank}(M_k) = \sum_{k=0}^{m} (m-k+1+t) = \frac{(m+1)(m+2t+2)}{2}, \tag{6}$$

and its determinant is $\det(\mathcal{L}) = B^s X^{s_x} Y^{s_y} = \prod_{k=0}^{m} \det(M_k)$. We get easily

$$s = \sum_{k=0}^{m} s_{B,k} = \frac{m(m+1)(2m+3t+4)}{6} = \frac{1}{3}m^3 + \frac{1}{2}m^2 t + o(m^3),$$
$$s_x = \sum_{k=0}^{m} s_{x,k} = \frac{m(m+1)(2m+3t+4)}{6} = \frac{1}{3}m^3 + \frac{1}{2}m^2 t + o(m^3),$$
$$s_y = \sum_{k=0}^{m} s_{y,k} = \frac{(m+1)(m^2+3tm+2m+3t^2+3t)}{6} = \frac{1}{6}m^3 + \frac{1}{2}m^2 t + \frac{1}{2}mt^2 + o(m^3).$$

Applying Theorem 4.1 with $i = 2$, the LLL algorithm outputs two short polynomials $h_1(x,y)$ and $h_2(x,y)$ satisfying

$$\|h_1(x,y)\|, \|h_2(x,y)\| \leq 2^{\frac{n}{4}} \det(\mathcal{L})^{\frac{1}{n-1}}$$

Since $h_1(x,y) \equiv h_2(x,y) \equiv 0 \pmod{B^m}$, then, in order to apply Howgrave-Graham's theorem 4.2, a sufficient condition is $2^{\frac{n}{4}} \det(\mathcal{L})^{\frac{1}{n-1}} \leq \frac{B^m}{\sqrt{n}}$, which transforms to

$$\det(\mathcal{L}) \leq \frac{2^{-\frac{n(n-1)}{2}}}{n^{\frac{n-1}{4}}} \cdot B^{m(n-1)}.$$

Since $\det(\mathcal{L}) = B^s X^{s_x} Y^{s_y}$ with $X = B^\delta$, $Y = B^\beta$, we get

$$B^{s+\delta s_x+\beta s_y} \leq \frac{2^{-\frac{n(n-1)}{2}}}{n^{\frac{n-1}{2}}} \cdot B^{m(n-1)}. \tag{7}$$

Notice that $\frac{2^{-\frac{n(n-1)}{2}}}{n^{\frac{n-1}{2}}} = B^{-\varepsilon_1}$ for some small constant $\varepsilon_1 > 0$ which can be ignored. On the other hand, ignoring the low terms in s, s_x and s_y and using $m(n-1) = \frac{1}{2}m^3 + m^2 t + o(m^3)$, we get

$$s + \delta s_x + \beta s_y = \frac{2+2\delta+\beta}{6}m^3 + \frac{1+\delta+\beta}{2}m^2 t + \frac{\beta}{2}mt^2,$$

and the condition (7) can be rewritten as

$$\frac{2+2\delta+\beta}{6}m^3 + \frac{1+\delta+\beta}{2}m^2 t + \frac{\beta}{2}mt^2 < \frac{1}{2}m^3 + m^2 t,$$

or equivalently

$$\frac{-1+2\delta+\beta}{6}m^2 + \frac{-1+\delta+\beta}{2}mt + \frac{\beta}{2}t^2 < 0.$$

Optimizing with respect to t, we get for $t = \frac{1-\delta-\beta}{2\beta}m$

$$\frac{m^2}{24\beta}\left(-3\delta^2 + (6+2\beta)\delta + \beta^2 + 2\beta - 3\right) < 0.$$

Hence, we must have $-3\delta^2 + (6+2\beta)\delta + \beta^2 + 2\beta - 3 < 0$, that is $\delta < 1 + \frac{1}{3}\beta - \frac{2}{3}\sqrt{\beta^2 + 3\beta}$. Under this condition, the polynomials $h_1(x,y)$ and $h_2(x,y)$ share the solution (x_0, y_0) which can be obtained by extracting the roots of the resultant polynomial over the integers. This terminates the proof. □

4.3 Lattice-reduction cryptanalysis of RSA

A number of lattice attacks on RSA Cryptosystem are motivated by the LLL algorithm and Coppersmith's techniques for solving polynomial equations. In this section we consider some attacks on RSA that are related to lattice methods (see (Boneh, 1999), (Hinek, 2009) and the references therein for detailed information).

4.3.1 Factoring the RSA modulus with partial knowledge of p

In (Coppersmith, 1997), Coppersmith presented a method which enables us to factor the modulus $N = pq$ in time polynomial in its bitsize provided that we know half of the bits of p. The original method is based in small roots of bivariate polynomial equations. We present a variant which is based on univariate modular polynomial equations (see (Howgrave-Graham, 2001) and (May, 2003)). We begin by the most significant bits of p case.

Theorem 4.7. *Let $N = pq$ be an RSA modulus with $p > q$. Furthermore, let k be an (unknown) integer that is not a multiple of q. Suppose we know an approximation $\tilde{p}$ of kp such that $|kp - \tilde{p}| < N^{\frac{1}{4}}$. Then we can find the factorization of N in time polynomial in $\log N$.*

Proof. Write $x_0 = kp - \tilde{p}$ and $f_p(x) = \tilde{p} + x$. Then $f_p(x_0) = kp \equiv 0 \pmod{p}$ with $p > N^{\frac{1}{2}}$. We can then apply Coppersmith's theorem 4.4 with $d = 1$, $\beta = \frac{1}{2}$ and $c_N = 1$ and get the root x_0 since $|x_0| < N^{\frac{1}{4}}$. Hence $kp = x_0 + \tilde{p}$ and $\gcd(kp, N) = p$ since $k \not\equiv 0 \pmod{q}$. □

We can obtain a similar result for the case where we know the less significant bits of p.

Theorem 4.8. *Let $N = pq$ be an RSA modulus with $p > q$. Let k be an (unknown) integer that is not a multiple of q. Suppose we know M and p_0 such that $kp \equiv p_0 \pmod{M}$ with $M > kpN^{-\frac{1}{4}}$. Then we can find the factorization of N in time polynomial in $\log N$.*

Proof. Write $x_0 = \frac{kp - p_0}{M}$ and $f_p(x) = Mx + p_0$. Then $f_p(x_0) = kp \equiv 0 \pmod{p}$. Suppose $M > kpN^{-\frac{1}{4}}$. Then

$$x_0 = \frac{kp - p_0}{M} < \frac{kp}{M} < N^{\frac{1}{4}}.$$

We can then apply Coppersmith's theorem 4.4 with $d = 1$, $\beta = \frac{1}{2}$ and $c_N = 1$ and get the root x_0. Hence p can be found by $\gcd(kp, N) = p$ where $kp = Mx_0 + p_0$. □

4.3.2 Factoring the RSA modulus with small prime difference

Let $N = pq$ be an RSA modulus with $q < p < 2q$ and small prime difference $p - q < N^{\frac{1}{4}}$. In (Weger, 2002), de Weger showed how to factor N using Fermat's method of factoring. We present below an alternate method based on Coppersmith's technique.

Theorem 4.9. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. If $p - q < N^{\frac{1}{4}}$, then we can find the factorization of N in time polynomial in $\log N$.*

Proof. Suppose $q < p < 2q$ and $p - q < N^{\frac{1}{4}}$. Then, using Lemma 3.2, we get

$$\sqrt{N} < p < q + N^{\frac{1}{4}} < \sqrt{N} + N^{\frac{1}{4}}.$$

Hence $0 < p - \sqrt{N} < N^{\frac{1}{4}}$ and by Theorem 4.7, this leads to the factorization of N. □

4.3.3 Boneh and Durfee's class of weak keys

In 1999, Boneh and Durfee(Boneh & Durfee, 1999) introduced the small inverse problem and presented a substantial improvement over Wiener's bound. Their attack can recover the primes p, q in polynomial time provided that $d < N^{0.292}$. Their result is is based on Coppersmith's technique for finding small solutions to modular polynomial equations. We present a weaker result which is valid for $d < N^{0.284}$.

Theorem 4.10. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $e < \phi(N)$ be a public exponent and d be the corresponding private exponent. If $d < N^{0.284}$, then, under Assumption 1, we can find the factorization of N in time polynomial in $\log N$.*

Proof. Starting with the equation $ed - k\phi(N) = 1$, we get $k(N + 1 - p - q) + 1 = ed$ which leads to the modular equation $x(A + y) + 1 \equiv 0 \pmod{e}$, where $A = N + 1$. This is an inverse problem with the solution $(k, -p - q)$. Suppose $e < \phi(N)$ is of the same order of magnitude as N, that is $e \approx N$. If $d < N^{\delta}$, we get $k = \frac{ed-1}{\phi(N)} < \frac{ed}{\phi(N)} < d < N^{\delta}$. On the other hand, since $q < p < 2q$, then $p + q = \mathcal{O}\left(N^{\frac{1}{2}}\right)$. Using Theorem 4.6 with $B = e$ and $\beta = \frac{1}{2}$, we can solve the equation $x(A + y) + 1 \equiv 0 \pmod{e}$, with $|x| < X = N^{\delta}$ and $|y| < Y = N^{\beta}$ provided that

$$\delta < 1 + \frac{1}{3}\beta - \frac{2}{3}\sqrt{\beta^2 + 3\beta} = \frac{7}{6} - \frac{1}{3}\sqrt{7} \approx 0.284.$$

Using $p + q = y$, we can get p and q easily. This terminates the proof. □

4.3.4 Another generalization of Wiener's attack on RSA

Suppose e satisfies an equation $ex - (N + 1 - ap - bq) = 1$ where $\frac{a}{b}$ is an unknown approximation of $\frac{q}{p}$. We recall that this means that $a = \left[\frac{bq}{p}\right]$ (where $[x]$ denotes the closest integer to the real number x). In Section 3.2.3, we presented an attack, based on continued fractions that enables us to find the factorization of N if $xy < \frac{N}{2(ap+bq)}$. We present below an alternate attack based on the small inverse problem.

Theorem 4.11. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $\frac{a}{b}$ be an unknown approximation of $\frac{q}{p}$ and e be a public exponent satisfying an equation $ex - (N + 1 - ap - bq)y = 1$ with $|y| < e^{\delta}$ and $|ap + bq| < e^{\frac{1}{2}+\alpha}$. If*

$$\delta < \frac{7}{6} + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{4\alpha^2 + 16\alpha + 7},$$

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

Proof. We rewrite the equation $ex - (N + 1 - ap - bq)y = 1$ as an inverse equation $(N + 1 + z)y + 1 \equiv 0 \pmod{e}$, where $z = -ap - bq$. Let $Y = e^{\delta}$ and $Z = e^{\beta}$. We have to find y and z such that $(N + 1 + z)y + 1 \equiv 0 \pmod{e}$ with $|y| < Y$ and $|z| < Z$. Using Theorem 4.6 with $B = e$ and $\beta = \frac{1}{2} + \alpha$, we can solve the equation $y(N + 1 + z) + 1 \equiv 0 \pmod{e}$, with $|y| < Y = e^{\delta}$ and $|z| < Z = e^{\beta}$ provided that $\delta < 1 + \frac{1}{3}\beta - \frac{2}{3}\sqrt{\beta^2 + \beta}$. Using $\beta = \frac{1}{2} + \alpha$, we get

$$\delta < \frac{7}{6} + \frac{1}{3}\alpha - \frac{1}{3}\sqrt{4\alpha^2 + 16\alpha + 7}.$$

With $z = -ap - bq$, we find p using the same technique as in Theorem 3.6. □

4.3.5 Least significant bits of d known: the attack of Blömer and May

In (Blömer & May, 2003), Blömer and May presented an attack on RSA with a private exponent d for which the least significant bits are known.

Theorem 4.12 (Blömer-May). *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let e be a public exponent with $e = N^{\alpha}$ and $\alpha < \frac{1}{2}$. Let d be the secret exponent satisfying $ed - k\phi(N) = 1$. If we know d_0 and M such that $d \equiv d_0 \pmod M$ and $M = N^{\frac{1}{2}+\alpha+\varepsilon}$ for $\varepsilon > 0$, then the factorization of N can be found in polynomial time.*

Proof. Suppose we know d_0 and M such that $d \equiv d_0 \pmod M$. Then $d = Mx_0 + d_0$ where x_0 is the unknown part of d. Since $ed - k\phi(N) = 1$, then $eMx_0 + ed_0 - k(N + 1 - p - q) = 1$ and $eMx_0 + k(p + q - 1) + ed_0 - 1 = kN$. This gives us a bivariate linear polynomial equation $eMx + y + ed_0 - 1 \equiv 0 \pmod N$, with the solution $x = x_0$ and $y = y_0 = k(p + q - 1)$. Let $M = N^{\frac{1}{2}+\alpha+\varepsilon}$. We have $d = Mx_0 + d_0 < N$, then $x_0 < \frac{N}{M} = N^{\frac{1}{2}-\alpha-\varepsilon}$. We then set $X = N^{\frac{1}{2}-\alpha-\varepsilon}$ for $\alpha < \frac{1}{2}$. On the other hand, we have $k = \frac{ed-1}{\phi(N)} < \frac{ed}{\phi(N)} < e = N^{\alpha}$. Hence $y_0 = k(p + q - 1) < N^{\frac{1}{2}+\alpha}$. We set $Y = N^{\frac{1}{2}+\alpha}$ and apply Theorem 4.5 with $\beta = 1$, $|x_0| < X$ and $|y_0| < Y$. We find a solution (x_0, y_0) if

$$\frac{1}{2} - \alpha - \varepsilon + \frac{1}{2} + \alpha < 3\beta - 2 + 2(1-\beta)^{\frac{3}{2}} = 1,$$

which is satisfied for $\varepsilon > 0$. Using x_0 and y_0, we compute $d = Mx_0 + d_0$ and, since $eMx_0 + y_0 + ed_0 - 1 = kN$, we get

$$k = \frac{eMx_0 + y_0 + ed_0 - 1}{N}.$$

Plugging in the key equation $ed - k\phi(N) = 1$, we obtain $\phi(N) = \frac{ed-1}{k}$ which leads to the factorization of N. □

4.3.6 The Φ-Hiding Assumption

The Φ-Hiding Assumption states that it is computationally untractable to decide whether a given small prime e divides $\phi(N)$ where N is a composite integer with unknown factorization. The Φ-Hiding Assumption has been introduced by Cachin, Micali and Stadler (Cachin et al., 1999) and has found various applications in cryptography. We present a solution of the Φ-Hiding Assumption when the composite integer is an RSA modulus $N = pq$ or an RSA multi-prime $N = p_1p_2p_3$.

Theorem 4.13. *Let $N = pq$ be an RSA modulus with $q < p$ and e be a prime integer. If $e > N^{\frac{1}{4}+\varepsilon}$, then the Φ-Hiding Assumption is solvable in polynomial time.*

Proof. If e is prime and divides $\phi(N) = (p-1)(q-1)$, then e divides $(p-1)$ or $(q-1)$. Suppose e divides $p - 1$. Then there exist a positive integer x_0 such that $ex_0 = p - 1$ which implies $ex_0 + 1 \equiv 0 \pmod p$. If $e > N^{\frac{1}{4}+\varepsilon}$, then using Lemma 3.2, we get

$$x_0 = \frac{p-1}{e} < \frac{p}{e} < \frac{\sqrt{2}N^{\frac{1}{2}}}{N^{\frac{1}{4}+\varepsilon}} = N^{\frac{1}{4}-\varepsilon'},$$

for some small ε'. Hence, using Coppersmith's Theorem 4.3 with $\beta = \frac{1}{2}$ and $\delta = 1$, we can find x_0 and then solve the Φ-Hiding Assumption. □

For a multi-prime RSA modulus of the form $N = pqr$, the Φ-Hiding Assumption assumes that deciding whether a prime e is a divisor of $p-1$ and $q-1$ or not is hard. For a general multi-prime RSA modulus $N = p_1 \dots p_n$, see Herrmann's work (Herrmann, 2011).

Theorem 4.14. *Let $N = pqr$ be a multi-prime RSA modulus with $r < q < p$ and e be a prime integer. If $e > N^{\frac{1}{2}-\frac{2\sqrt{3}}{27}}$, then the Φ-Hiding Assumption is solvable in polynomial time.*

Proof. Let $e = N^{\alpha}$. Suppose e divides $p-1$ and $q-1$. Then $ex + 1 = p$ and $ey + 1 = q$ for some positive integers x and y satisfying $x, y < \frac{p}{e} < N^{\frac{1}{2}-\alpha}$. Multiplying and expanding the equations, we get $e^2xy + e(x+y) + 1 = pq$, with $pq > N^{\frac{2}{3}}$. To apply Theorem 4.5 with the equation $e^2u + ev + 1 \equiv 0 \pmod{pq}$, where $u = xy < N^{1-2\alpha}$, $v = x + y = 2N^{\frac{1}{2}-\alpha} = N^{\frac{1}{2}-\alpha+\varepsilon}$, a sufficient condition is that

$$1 - 2\alpha + \frac{1}{2} - \alpha < 3\beta - 2 + 2(1-\beta)^{\frac{3}{2}}$$

where $\beta = \frac{2}{3}$. This gives the condition $\alpha > \frac{1}{2} - \frac{2\sqrt{3}}{27}$, and consequently $e > N^{\frac{1}{2}-\frac{2\sqrt{3}}{27}}$. □

5. Diophantine and Lattice cryptanalysis of RSA

In this section we present two attacks on RSA that combine continued fractions and Coppersmith's lattice based technique.

5.1 Blömer and May's class of weak keys

We consider the class of public keys (N, e) satisfying an equation $ex - y\phi(N) = z$. In 2004, Blömer and May (Blömer & May, 2004) showed that using such exponents makes RSA insecure if $N = pq$ with $p - q = cN^{\frac{1}{2}}$ for some constant $0 < c \le 1$ and

$$0 \le x \le \frac{1}{3}\sqrt{\frac{\phi(N)}{e}\frac{N^{\frac{3}{4}}}{p-q}} \quad \text{and} \quad |z| \le \frac{p-q}{\phi(N)N^{\frac{1}{4}}} \cdot ex.$$

We reformulate this attack in the following result where the primes p and q can be unbalanced.

Theorem 5.1. *Let (N, e) be an RSA public key tuple with $N = pq$ and $q < p$. Suppose that e satisfies an equation $ex - y\phi(N) = z$ with $\gcd(x, y) = 1$ and*

$$xy < \frac{N}{4(p+q)} \quad \text{and} \quad |z| < \frac{(p-q)N^{\frac{1}{4}}y}{3(p+q)}.$$

Then N can be factored in polynomial time.

Proof. Rewrite $ex - y\phi(N) = z$ as $ex - yN = z - y(p+q-1)$. Then

$$\left|\frac{e}{N} - \frac{y}{x}\right| = \frac{|z - y(p+q-1)|}{Nx} \le \frac{|z| + y(p+q-1)}{Nx}. \tag{8}$$

Suppose $\gcd(x, y) = 1$ and $|z| < \frac{(p-q)N^{\frac{1}{4}}y}{3(p+q)}$ then $|z| < N^{\frac{1}{4}}y$. Hence

$$|z| + (p+q+1)y| \le N^{\frac{1}{4}}y + (p+q+1)y = (N^{\frac{1}{4}} + p + q + 1)y < 2(p+q)y.$$

Plugging in (8), we get $\left|\frac{e}{N}-\frac{y}{x}\right| < \frac{2(p+q)y}{Nx}$. Now, assume that $xy < \frac{N}{4(p+q)}$. Then $\frac{2(p+q)y}{Nx} < \frac{1}{2x^2}$ which implies $\left|\frac{e}{N}-\frac{y}{x}\right| < \frac{1}{2x^2}$. Then, by Theorem 3.1, $\frac{y}{x}$ is a convergent of the continued fraction of $\frac{e}{N}$. Using x and y, define

$$U = N+1-\frac{ex}{y}, \qquad V=\sqrt{|U^2-4N|}.$$

Transforming the equation $ex-(p-1)(q-1)y=z$ into $p+q-\left(N+1-\frac{ex}{y}\right)=\frac{z}{y}$, we get

$$|p+q-U| = \left|p+q-\left(N+1-\frac{ex}{y}\right)\right| = \frac{|z|}{y} < \frac{(p-q)N^{\frac{1}{4}}}{3(p+q)} < N^{\frac{1}{4}}. \tag{9}$$

Now, we have

$$\left|(p-q)^2-V^2\right| = \left|(p-q)^2-\left|U^2-4N\right|\right| \le \left|(p-q)^2-U^2+4N\right| = \left|(p+q)^2-U^2\right|$$

Dividing by $p-q+V$, we get

$$|p-q-V| \le \frac{\left|(p+q)^2-U^2\right|}{p-q+V} = \frac{|p+q-U|\,(p+q+U)}{p-q+V}. \tag{10}$$

Observe that (9) implies $p+q+U < 2(p+q)+N^{\frac{1}{4}} < 3(p+q)$. On the other hand, we have $p-q+V > p-q$. Plugging in (10), we get

$$|p-q-V| < \frac{3(p+q)(p-q)N^{\frac{1}{4}}}{3(p+q)(p-q)} = N^{\frac{1}{4}}.$$

Combining this with (9), we deduce

$$\left|p-\frac{U+V}{2}\right| = \left|\frac{p+q}{2}-\frac{U}{2}+\frac{p-q}{2}-\frac{V}{2}\right| \le \left|\frac{p+q}{2}-\frac{U}{2}\right| + \left|\frac{p-q}{2}-\frac{V}{2}\right| < N^{\frac{1}{4}}.$$

Hence $\frac{U+V}{2}$ is an approximation of p up to an error term of at most $N^{\frac{1}{4}}$. Then Coppersmith's Theorem 4.7 will find p in polynomial time and the factorization of N follows. □

5.2 Another class of weak keys

Let $N = pq$ be an RSA modulus with $q < p < 2q$ and e be a public exponent. Suppose e satisfies an equation $ex-(N-up-v)y=z$. We present below an attack on RSA with such exponents when the unknown parameters x, u, v, y and z are suitably small.

Theorem 5.2. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let e be a public exponent satisfying an equation $ex-(N-up-v)y=z$ with $\gcd(x,y)=1$ and*

$$xy < \frac{N}{4|up+v|} \quad \textit{and} \quad |z| \le |up+v|y \quad \textit{and} \quad \left|v-\frac{z}{y}\right| < N^{\frac{1}{4}}.$$

Then N can be factored in polynomial time.

Proof. We rewrite the equation $ex-(N-up-v)y=z$ as $ex-Ny=z-(up+v)y$ and divide by Nx. We get

$$\left|\frac{e}{N}-\frac{y}{x}\right|=\frac{|z-(up+v)y|}{Nx}\leq\frac{|z|+|up+v|y}{Nx}.$$

If we suppose $|z|\leq|up+v|y$, we get $\left|\frac{e}{N}-\frac{y}{x}\right|\leq\frac{2|up+v|y}{Nx}$. Next, if $xy<\frac{N}{4|up+v|}$, then $\frac{2|up+v|y}{Nx}<\frac{1}{2x^2}$. Hence $\left|\frac{e}{N}-\frac{y}{x}\right|\leq\frac{1}{2x^2}$, which implies, by Theorem 3.1, that $\frac{y}{x}$ is a convergent of the continued fraction expansion of $\frac{e}{N}$. Using x and y in the equation $ex-(N-up-v)y=z$, we get $up=N-\frac{ex}{y}+\frac{z}{y}-v$. If $\left|v-\frac{z}{y}\right|<N^{\frac{1}{4}}$, then $\left|up-N+\frac{ex}{y}\right|<N^{\frac{1}{4}}$. Hence $N-\frac{ex}{y}$ is an approximation of up up to an additive term at most $N^{\frac{1}{4}}$. Using Coppersmith's technique of Theorem 4.7, this leads to the factorization of N. □

6. Conclusion

In this study, we have examined the RSA cryptosystem, the most widely deployed public-key cryptosystem. We have also studied various cryptanalytic attacks on RSA and presented the main algebraic tools to follow the attacks. Specifically, we contributed the following to the field of the RSA cryptosystem study:

- We described the main schemes of RSA, namely key generation, encryption and decryption.
- We provided a detailed survey of the mathematical algebraic tools that are used in the principal attacks on RSA. This includes continued fractions and Diophantine approximations, the basic theory of lattices and the LLL algorithm for basis reduction as well as the theory of finding small solutions of modular polynomial equations.
- We presented new attacks on RSA and revisited various old ones that are based on Diophantine approximations, lattice reduction and Coppersmith's techniques for solving modular polynomial equations.

The effectiveness of the proposed attacks is optimized for instances of RSA with small private exponents or public exponents satisfying some specific equations. These results illustrate once again the fact that the crypto-designer should be very cautious when using RSA with such secret exponents.

7. References

Ajtai, M. (1998). The Shortest Vector Problem in L2 is NP-hard for Randomized Reductions, In *STOC*, pp. 10-19.

Blömer, J. & May, A. (2004). A generalized Wiener attack on RSA, In *Public Key Cryptography - PKC 2004*, volume 2947 of LNCS, pp. 1-13. Springer-Verlag.

Blömer, J. & May, A. (2003). New Partial Key Exposure Attacks on RSA, *Proceedings of CRYPTO 2003, LNCS* 2729 [2003], pp. 27-43. Springer Verlag.

Boneh, D. (1999). Twenty years of attacks on the RSA acyptosystem, *Notices of the AMS* 46 (2) (February 1999) pp. 203-213.

Boneh, D. & Durfee, G. (1999). Cryptanalysis of RSA with private key d less than $N^{0.292}$, *Advances in Cryptology, Eurocrypt'99, LNCS* Vol. 1592, pp. 1-11, Springer-Verlag.

Cachin, C.; Micali, S. & Stadler, M. (1999). Computationally Private Information Retrieval with Polylogarithmic Communication, In *EUROCRYPT*, pp. 402-414, Springer-Verlag.

Cohen, H. (1993). *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, Vol. 138, Springer-Verlag, 1993.

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

Diffie, W. & Hellman, E. (1976). New directions in cryptography, *IEEE Transactions on Information Theory*, 22, 5 (1976), pp. 644-654.

Hardy, G. H.; & Wright, E. M. (1965). *An Introduction to the Theory of Numbers*, Oxford University Press, London.

Herrmann, M. (2008). Improved Cryptanalysis of the Multi-Prime Φ - Hiding Assumption, *A. Nitaj and D. Pointcheval (Eds.): AFRICACRYPT 2011, LNCS 6737*, pp. 92-99. Springer Verlag.

Herrmann, M. & May, A. (2008). Solving linear equations modulo divisors: On factoring given any bits, *J. Pieprzyk (Ed.): ASIACRYPT 2008, LNCS 5350*, pp. 406-424, Springer-Verlag.

Hinek, M. (2009). *Cryptanalysis of RSA and Its Variants*, Chapman & Hall/CRC, Cryptography and Network Security Series, Boca Raton, 2009.

Howgrave-Graham, N. (1997). Finding small roots of univariate modular equations revisited, In *Cryptography and Coding, LNCS 1355*, pp. 131-142, Springer-Verlag.

Howgrave-Graham, N. (2001). Approximate Integer Common Divisors, *CaLC 2001, LNCS* vol. 2146, pp. 51-66, Springer-Verlag.

Jochemsz, E. & May, A. (2006). A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, in: *ASIACRYPT 2006, LNCS*, vol. 4284, 2006, pp. 267-282, Springer-Verlag.

Lenstra, A. K.; Lenstra, H. W. & Lovász, L. (1982). Factoring polynomials with rational coefficients, *Mathematische Annalen*, Vol. 261, pp. 513-534.

May, A. (2003). *New RSA Vulnerabilities Using Lattice Reduction Methods*, Ph.D. thesis, Paderborn, 2003, `http://www.cits.rub.de/imperia/md/content/may/paper/bp.ps`

Nassr, D.I.; Bahig, H.M.; Bhery, A. & Daoud, S.S. (2008). A new RSA vulnerability using continued fractions. In *Proceedings of AICCSA*. 2008, pp. 694-701.

Rivest, R.; Shamir, A. & Adleman, L. (1978). A Method for Obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, Vol. 21 (2), pp. 120-126.

de Weger, B. (2002). Cryptanalysis of RSA with small prime difference, *Applicable Algebra in Engineering, Communication and Computing*, Vol. 13(1), pp. 17-28.

Wiener, M. (1990). Cryptanalysis of short RSA secret exponents, *IEEE Transactions on Information Theory*, Vol. 36, pp. 553-558.