On the Multiple Fault Attack on RSA Signatures with LSBs of Messages Unknown *

Lidong Han, Wei Wei, Mingjie Liu
Institute for Advanced Study
Tsinghua University, Beijing 100084, China
hanlidong@mail.tsinghua.edu.cn
wei-wei08,liu-mj07@mails.tsinghua.edu.cn

Abstract. In CHES 2009, Coron, Joux, Kizhvatov, Naccache and Paillier (CJKNP) introduced a fault attack on RSA signatures with partially unknown messages. They factored RSA modulus N using a single faulty signature and increased the bound of unknown messages by multiple fault attack, however, the complexity multiple fault attack is exponential in the number of faulty signatures. At RSA 2010, it was improved which run in polynomial time in number of faults.

Both previous multiple fault attacks deal with the general case that the unknown part of message is in the middle. This paper handles a special situation that some least significant bits of messages are unknown. First, we describe a sample attack by utilizing the technique of solving simultaneous diophantine approximation problem, and the bound of unknown message is $N^{\frac{1}{2}-\frac{1}{2\ell}}$ where ℓ is the number of faulty signatures. Our attacks are heuristic but very efficient in practice. Furthermore, the new bound can be extended up to $N^{\frac{1}{2}^{1+\frac{1}{\ell}}}$ by the Cohn-Heninger technique. Comparison between previous attacks and new attacks with LSBs of message unknown will be given by simulation test.

Key words: Fault Attacks,RSA Signatures, Least Significant Bits (LSBs), ISO/IEC 9796-2, LLL Algorithm

1 Introduction

RSA signature [13] invented by Rivest, Shamir and Adleman is the most popular digital signature scheme. To sign a message m, the signer first encodes m as $\mu(m)$ using the encoding function $\mu(\cdot)$, then computes $\rho = \mu(m)^d \mod N$, which is the signature of the message m. To verify the signature, the receiver checks that the following equation holds:

* Supported by the National Natural Science Foundation of China (No.61133013) and the Tsinghua University Initiative Scientific Research Program (No.20111080970).

$\rho^e = \mu(m) \mod N$ holds. A sophisticated way to speed up the signature generation is to exploit the Chinese Remainder Theorem (CRT). This is done by computing:

$$\rho_p = \mu(m)^{d_p} \mod p \text{ and } \rho_q = \mu(m)^{d_q} \mod q,$$

where $d_p = d \pmod{p-1}$ and $d_q = d \pmod{q-1}$. We obtain the signature

$$\rho = \rho_p + p \cdot (p^{-1} \mod q) \cdot (\rho_q - \rho_p) \mod N$$

using CRT. Such an approach, called RSA-CRT, achieves the signing time that is approximately four times faster than signature using the standard RSA definition.

The first fault attack against RSA-CRT signature implementation was introduced by Boneh, DeMillo and Lipton [1] in 1997. In the fault attack, we assume the attacker has the ability to induce a fault when computing the signature by CRT and only one of the above computations is fault, e.g.,

$$\rho^e = \mu(m) \mod p \text{ and } \rho^e \neq \mu(m) \mod q.$$

Hence, if the encoding function is public, RSA modulus N can be factored by computing

$$\gcd(\rho^e - \mu(m) \mod N, N) = p. \tag{1}$$

In ISO/IEC 9796-2 the encoding function is the form:

$$\mu(m) = 6A_{16}||m[1]||H(m)||BC_{16}$$

where $m = m[1]||m[2]$ is split into two parts. In [4], Coron, Joux, Kizhvatov, Naccache and Paillier (CJKNP) proposed fault attack against RSA signature with unknown message part (UMP). CJKNP's attack can factor the RSA modulus N using a single faulty signature and they extended the attack to multiple faulty signatures, however the time complexity is exponential in the number of faulty signatures. At RSA 2010, Coron, Naccache and Tibouchi (CNT) in [6] exhibited a simpler multiple fault attack, whose complexity is polynomial in number of faulty signatures.

Both previous attacks can be applied to any signed messages with unknown part in the middle. In conclusion of [4], CJKNP point out the single fault attack can be used to the PKCS#1 v1.5 encoding where the unknown part locates on some least significant bits. However, multiple fault attacks in [4, 6] don't analyze the scenario when the unknown part of message occurs the least significant bits.

In this paper, we will reconsider the fault attacks against the randomized version of ISO/IEC 9796-2, and the partially unknown part of message $m[1]$ is located in the least significant bits (LSBs). For example, the ”stereotyped” message $m[1]$ is ”On April 16, 2012, the secret key for this day is ... ”. If the unknown part is relatively long, both previous attacks may be invalid. Our main goal is to extend the bound of the unknown part of the message using the multiple faulty signature. Based on solving simultaneous Diophantine approximation problem, the multiple faulty attack can heuristically factor N if the unknown part is at most $N^{\frac{1}{2}-\frac{1}{2\ell}}$, where ℓ is the number of faulty signatures, while the previous bound in [6] is $N^{\frac{1}{2}-\frac{2}{\ell}}$.

In addition, when the number of faulty signatures is large, the bound of unknown part can be improved up to $N^{\frac{1}{2}^{1+\frac{1}{\ell}}}$ based on the technique presented by Cohn and Heninger. Although our new attack is heuristic, it works well in practice and paradoxically becomes more efficient as the modulus bit-length increases. It is noted that the new attack is not suit for EMV signatures. We hope that the new attack can be helpful to other signature schemes.

The rest of this paper is organized as follows. Section 2 gives a simple description of ISO/IEC 9796-2, and recall the CJKNP's attack. In section 3, for completeness, we first describes a single fault attack in detail when some LSBs of $m[1]$ are unknown, and then present the multiple fault attack in a simple way and improve the bound of the unknown part of messages. In last subsection, we indicate that the bound can be extended directly by Cohn-Heninger results. Finally, we give some simulation results and compare the new attacks with the previous attacks in section 4.

2 CJKNP's Attack on ISO/IEC 9796-2

2.1 ISO/OEC 9796-2 Standard

ISO/IEC 9796-2 is an encoding standard allowing partial or total message recovery [10, 11]. In the following, we introduce ISO/IEC 9796-2 as in [7, 6]. The encoding function can be used as a hash function $H(m)$ of digest size k_h. For the sake of simplicity we assume that k_h, the size of m and the size of N (denoted by k) are all multiples of 8. The ISO/IEC 9796-2 encoding of a message $m = m[1]||m[2]$ is

$$\mu(m) = 6A_{16}||m[1]||H(m)||BC_{16}$$

where $m[1]$ consists of the $k - k_h - 16$ most significant bits of m and $m[2]$ represents the remaining bits of m. Recently, some attacks against

ISO/IEC 9796-2 are proposed in [5, 7] by Coron *et al*, especially [7] gave a practical forgery attack (without faults).

2.2 CJKNP's Single Fault Attack

In 2009, CJKNP described a fault attack on a randomized version of ISO/IEC 9796-2 standard. More precisely, the authors in [4] analyzed a message $m = m[1]||m[2]$ of the form

$$m[1] = \alpha||r||\alpha', \quad m[2] = \text{DATA}$$

where r is an unknown part, α, α' are known and DATA is some known or unknown string. The size of r is denoted by k_r and the size of $m[1]$ is $k - k_h - 16$ as required in ISO/IEC 9796-2. The encoded message can be written as

$$\mu(m) = 6A_{16}||\alpha||r||\alpha'||H(\alpha||r||\alpha'||\text{DATA})||BC_{16}. \qquad (2)$$

The total number of unknown bits in $\mu(m)$ is $k_r + k_h$. Assume that the attacker can obtain a faulty signature satisfying (1), then from (1) and (2) one can get

$$\rho^e = s + r \cdot 2^{n_r} + H(m) \cdot 2^8 \mod p,$$

where s is a known value, and $n_r = k_h + k_{\alpha'} + 4$ (the size of α' is denoted by $k_{\alpha'}$). This shows that $(r, H(m))$ must be a solution of the equation

$$a + bx + cy = 0 \mod p$$

where $a := s - \rho^e \mod N, b := 2^{n_r}$ and $c := 2^8$ are known. This problem can be solved using the result of Herrmann and May in [8] based on Coppersmith's method [3] for finding small roots of polynomial equations. Assuming that $r < N^\gamma$, $H(m) < N^\delta$, one can find r and $H(m)$ under the condition:

$$\gamma + \delta \leq \frac{\sqrt{2} - 1}{2} \approx 0.207$$

for a balanced RSA modulus.

3 Attacks against ISO/IEC 9796-2 with MSBs of message known

The single fault attack against the signature scheme with some LSBs of message unknown such as the PKCS#1 v1.5 encoding was mentioned in [4]. However, multiple fault attack for such case has not been discussed.

In the following, we will give an analysis of multiple fault attack with some LSBs of message unknown. For completeness of this paper, we will first describe the single fault attack against a probabilistic variant of the ISO/IEC 9796-2 in detail in subsection 3.1. And two faults modulo different factors will be discussed in subsection 3.2. The last two subsections present the multiple fault attack against the randomized version of ISO/IEC 9796-2.

3.1 Single Fault Attack

Assume that some least significant bits of message $m[1]$ are unknown. That is

$$m[1] = \alpha || r, \quad m[2] = \text{DATA}$$

The size of unknown part r is denoted as k_r and the size of $m[1]$ is $k - k_h - 6$ as required in ISO/IEC 9796-2. The encoded message is then

$$\mu(m) = 6A_{16} || \alpha || r || H(\alpha || r || \text{DATA}) || BC_{16}. \tag{3}$$

The total number of unknown bits in $\mu(m)$ is $k_r + k_h$.

We suppose that after injecting a fault the opponent is in possession of a faulty signature ρ such that

$$\rho^e = \mu(m) \mod p, \quad \rho^e \neq \mu(m) \mod q. \tag{4}$$

From (3) we can write

$$\mu(m) = s + r' \cdot 2^8$$

where $s = (6A_{16} || \alpha) \cdot 2^{k_r + k_h + 8} + BC_{16}$ is a known value and $r' = r \cdot 2^{k_h} + H(m)$ is unknown. From (4) we obtain

$$\rho^e = s + r' \cdot 2^8 \mod p.$$

This shows that $x_0 = r \cdot 2^{k_h} + H(m)$ must be a solution of the equation

$$a + bx = 0 \mod p, \tag{5}$$

where $a := s - \rho^e \mod N, b := 2^8$ are known. Note that we can assume $b = 1$ by multiplying the equation by $b^{-1} \mod N$.

Therefore, if the root x_0 of the above equation can be found, one can obtain the factor p of N by computing GCD of N and $a + x_0$ from (5). This is a partially approximate common divisor problem, which can be solved using lattice technique by Howgrave-Graham [9].

Let X be the upper bound of the root x_0. From the result of [9], if $X < N^{\frac{1}{4}}$ one can factor the RSA modulus N. It means that for 1024-bit RSA modulus N, the total size of unknown x can be at most 256 bits. In our new attack, for ISO/IEC 9796-2 with $k_h = 160$, the size of the unknown lower bits of $m[1]$ can be as large as 96 bits. In our simulation tests in section 4, the new attack can work using the LLL algorithm [12] on 22 dimensional lattice in one second if r is a 83-bit number.

3.2 Two Faults Modulo Different Factors

In this subsection, we discuss the case that two faulty signatures modulo different factors are given. Assume that we have two faulty signatures ρ and ρ', such that $\rho^e = \mu(m) \mod p$ and $\rho'^e = \mu(m') \mod q$. From the analysis in the previous section, this gives two equations:

$$\begin{aligned} x_1 + a_1 &= 0 \mod p \\ x_2 + a_2 &= 0 \mod q \end{aligned}$$

where small unknowns x_1, x_2 are bounded by $x_1 \leq X_1, x_2 \leq X_2$ and $a_1, a_2 \leq N$. Multiplying the above two equations, we get a bivariate equation modulo N,

$$x_1 x_2 + a_2 x_1 + a_1 x_2 + a_1 a_2 = 0 \mod N.$$

Then x_1, x_2 can be solved by using the technique in [**?**] under the asymptotical condition $X_1 X_2 \leq N^{\frac{2}{3}}$. When $X_1 = X_2 = X$, the condition equals $X \leq N^{\frac{1}{3}}$. That is to say, if the total unknown part x containing the unknown part of message and hash function part is smaller than $N^{\frac{1}{3}}$, one can factor N efficiently given two faulty signatures modulo different factors.

3.3 Multiple Faults Modulo the Same Factor

CJKNP gave a multiple fault attack [4], whose complexity increases exponentially with the number of faulty signatures. In [6], the authors described a simpler multiple fault attack, in which the lattice dimension is the number of faults plus one, and gave a bound $\delta \leq \frac{1}{2} - \frac{2}{\ell}$. For more details we refer the reader to [6].

In order to improve the bound of the unknown part of random nonce, we will show how to extend to multiple faults. More precisely, given ℓ

faulty signatures, similar to analysis described in above, one has a collection of equations:

$$x_i + a_i = 0 \mod p, \quad \text{for } 1 \le i \le \ell \tag{6}$$

where a_i's are known and x_i's are unknown and small. Our goal is to recover the factor p.

In the following, we will adopt the technique of solving simultaneous Diophantine approximation problem. Let X be a suitable bound such that $x_i \le X$ for all $i \le \ell$. We construct the lattice $\mathcal{L}$ spanned by the rows of the following matrix

$$M = \begin{pmatrix} X & a_1 & a_2 & \dots & a_\ell \\ & N & & & \\ & & N & & \\ & & & \ddots & \\ & & & & N \end{pmatrix}$$

The dimension of the lattice $\mathcal{L}$ is $\ell + 1$ and the determinant of $\mathcal{L}$ is $N^\ell X$. From the Gaussian heuristic, the length of the smallest vector of the lattice $\mathcal{L}$ is roughly $\sqrt{\ell+1} \cdot (N^\ell X)^{\frac{1}{\ell+1}}$. From (6), there exist integers k_i for all $i \le \ell$ satisfying $a_i + x_i = k_i \cdot p$. Therefore, in the lattice $\mathcal{L}$, we have the vector $(qX, qx_1, qx_2, \cdots, qx_\ell) = (q, -k_1, -k_2, \cdots, -k_\ell) \cdot M$. Its Euclidean norm is approximately bounded by $\sqrt{\ell+1} \cdot qX$. If the bound is less than the heuristic shortest vector length, i.e., $qX \le (N^\ell X)^{\frac{1}{\ell+1}}$, it is very probable that the vector $(qX, qx_1, qx_2, \cdots, qx_\ell)$ in lattice $\mathcal{L}$ is the shortest vector. Assuming $X = N^\delta$, the condition is equal to

$$\delta \le \frac{1}{2} - \frac{1}{2\ell}. \tag{7}$$

It means that, if all x_i's in equation (6) satisfy $x_i \le N^{\frac{1}{2} - \frac{1}{2\ell}}$, the shortest vector $\mathbf{v}$ heuristically is unique by Minkowski theorem. Applying the lattice basis reduction algorithm to lattice of fixed dimension we obtain the shortest vector $\mathbf{v}$. This leads to factor N by computing GCD of the two first components of $\mathbf{v}$.

From the inequality (7), it is easy to see that the new bound is better than the former one in [6]. We will give some simulation and comparison in the next section.

3.4 Extended Multiple Fault Attack by Cohn-Heninger Technique

This subsection analyzes the multiple fault attack in order to improve the bound of unknown message part. Instead of using the above simple method of solving simultaneous Diophantine approximation problem, we now utilize the new technique by Cohn and Heninger[2].

In detail, assume we have a set of equations each of which is in form of $x_i + a_i = 0 \mod p$ and r_i is the solution of each equation. Our goal is to find polynomials in forms of $h(r_1, r_2, ..., r_\ell) = 0$. From Howgrave-Graham theorem, h satisfying two conditions is sufficient. Such two constrictions are:

1. $h(r_1, r_2, ..., r_\ell) = 0 \mod p^k$
2. $\|h(r_1, r_2, ..., r_\ell)\| < p^k/\sqrt{w}$, where $w = \deg(h)$

For the first one, we will compute such modulo polynomial as an integer linear combination of products

$$(x_1 + a_1)^{i_1} \cdots (x_\ell + a_\ell)^{i_\ell} N^\kappa$$

with $i_1 + \cdots + i_\ell + \kappa \geq k$. To ensure $\|h(r_1, r_2, ..., r_\ell)\| < p^k/\sqrt{w}$, we require h has small coefficients. It can be achieved to reduce a lattice with entries of polynomial coefficients. Let X be the upper bound of r_i. Use the polynomials

$$(X_1 x_1 + a_1)^{i_1} \cdots (X_\ell x_\ell + a_\ell)^{i_\ell} N^\kappa$$

to construct the lattice L, with $i_1 + \cdots + i_\ell + \kappa \leq t$ and $\ell = \max(k - \sum_j i_j, 0)$. The basis of the lattice consists of the ordering monomials and is an upper triangular matrix.

The dimension of L is

$$\dim L = \binom{t+\ell}{\ell}$$

and the determinant is

$$\det L = X^{\binom{t+\ell}{\ell}\frac{t\ell}{\ell+1}} N^{\binom{k+\ell}{\ell}\frac{k}{m+1}}$$

Applying a lattice reduction algorithm, we can get a reduced basis $v_1, v_2, ..., v_\ell$, such that

$$\|v_1\| \leq \cdots \leq \|v_\ell\| \leq 2^{\frac{\dim L(\dim L - 1)}{4(\dim + 1 - \ell)}} (\det L)^{\frac{1}{\dim L + 1 - \ell}}$$

If we require the left-hand side of above inequality is smaller than $p^k/\sqrt{\dim L}$, then the polynomials corresponding to $v_1, v_2, ..., v_\ell$ are equal to zero.

$$2^{\frac{\dim L(\dim L-1)}{4(\dim+1-\ell)}} (\det L)^{\frac{1}{\dim L+1-\ell}} \leq p^k/\sqrt{\dim L}$$

Neglecting all small terms, we have a asymptotical bound

$$(\det L)^{\frac{1}{\dim L+1-\ell}} \leq N^{\frac{1}{2}k}$$

Substituting the value of $\det L$ and optimizing the value of t, k, we get the Cohn-Heninger's result.

Theorem 1 (Cohn-Heninger [2].) *Given ℓ signatures $\rho_1, \rho_2, ..., \rho_\ell$ which are faulty signatures modulo p, and a bound X such that $|r_i| \leq X$ for all i, then RSA modulus N can be factored, provided that $X < N^{\frac{1}{2}^{1+\frac{1}{\ell}}}$ and the algebraic independence hypothesis holds. The complexity of the algorithm is polynomial in the number ℓ of faulty signatures.*

For $\ell = 1$, i.e., the attacker get only one faulty signature, the bound $X \leq N^{0.25}$ is same as the single faulty attack in subsection 3.1. If $\ell = 2$, the dimension of lattice is 36 with selecting $t = 7, k = 5$ as in [2], and the bound is about $N^{0.31}$. For all $\ell > 1$, the new bound is better than one in subsection 3.4. Although the dimension of lattice is large, the algorithm runs in polynomial time for fixed number ℓ.

4 Simulation Results

In this section we will only compare the known attacks and new attack by simulation. We have simulated the fault attacks described above as follows. Firstly, we generate a correct $\rho_p = \mu(m)^d \mod p$ and a random $\rho_q \in \mathbb{Z}_q$, then using CRT compute a faulty signature ρ with 160-bit Hash function. Secondly, we compute $(\rho^e - r)2^{-8} \mod N$ which is denoted as a, where s is a known value as in section 3.1. We use the NTL library [14] LLL algorithm on a 2Ghz Intel notebook.

Notice that, in our simulation tests, we only compare the new results with the previous attacks in [4, 6] under the assumption that UMP locates in the lower-order bits, although the attacks in [4, 6] can deal with the unknown bits in the middle.

4.1 Single-Fault Attack Simulations

In the following table, the simulation in Table 1 describes a single fault attack in [4]. The second table 1 simulates the new single fault attack in subsection 3.1. k is bit-size of RSA modulus N. k_r means the bit number of unknown message part. m, t is some parameters in lattice construction of subsection 3.1. w is the dimension of lattice.

Table 1. Single fault attack in [4]

modulus size k	UMP size k_r	m	t	ω	time
1024	6	10	3	66	4min
1024	13	13	4	105	51min
1536	70	8	2	45	39s
1536	90	10	3	66	9min
2048	158	8	2	45	55s

Table 2. New single fault attack

modulus size k	UMP size k_r	m	t	ω	time
1024	45	2	3	6	0.02s
1024	68	4	5	10	0.06s
1024	83	10	11	22	0.97s
1536	147	2	3	6	0.03s
1536	181	4	5	10	0.08s
1536	205	10	11	22	1.4s
2048	240	2	3	6	0.05s
2048	295	4	5	10	1.32s
2048	326	10	11	22	2.13s

For 1024-bit RSA modulus, in Table 1, when the UMP size k_r is 13, it requires more than 50 minutes to execute LLL algorithm on 105 dimensional lattice as in [4]. In fact, exhausting a 13-bit randomizer takes 0.13 seconds. For the same bit-size modulus in Table 2, k_r can be 83 by reducing only 22 dimensional lattice in one second, that can not be exhaustively searched in available time. For 2048-bit RSA modulus, the attack in Table 1 can deal with 158-bit UMP in more than one minute, while new attack can tackle 326-bit UMP in about two seconds.

Therefore, by comparing with the results in two tables, the new attacks can deal with more bits and are more efficient for larger moduli under our attacking scenario.

4.2 Multiple-Fault Attack Simulations

Table 3. Comparison of new multiple-fault attacks and previous attacks in [6]

ℓ	$\gamma + \delta_{theory,new}$	$\gamma + \delta_{true,new}$	$\gamma + \delta_{theory,[6]}$	$\gamma + \delta_{true,[6]}$
2	0.250	0.247	-	-
3	0.333	0.329	-	-
4	0.375	0.372	-	-
8	0.437	0.434	0.250	0.214
10	0.450	0.447	0.300	0.280
14	0.464	0.461	0.357	0.330
25	0.480	0.478	0.420	0.400
70	0.492	0.488	0.471	0.450

From Table 3, for small $\ell \leq 4$, in our simulation results, the new attacks can work well while the previous attacks in [6] are invalid since the bound $\delta < \frac{1}{2} - \frac{2}{\ell}$ is negative. Moreover, the asymptotic bound $\delta < \frac{1}{2} - \frac{1}{2\ell}$ in new attacks seems more natural.

For large ℓ, the new attack has the asymptotic bound closer to $\frac{1}{2}$ than former attacks, i.e., when $\ell = 70$, $k_r + k_h$ in [6] is 0.450 while one of new attack is 0.488. For a 1024-bit RSA modulus and 160-bit hash value, the new attack can deal with the 340-bit UMP better than 300-bit UMP in the previous attack. Therefore, the new attacks require less faulty signatures to deal with the same bound. And the value $\gamma+\delta$ in new results approaches to $\frac{1}{2}$ more fast.

From Table 3, another observation is that the difference between theoretical bound and test bound in new attack is much less than one in the previous attack, e.g, the distance in new attack is almost 0.03, however the distance provided by [6] is about 0.2.

Table 4. Extended Multiple-fault Attacks

ℓ	$\gamma + \delta$	t	k	w	time
2	0.310	7	5	36	15s
2	0.312	6	4	28	4s
3	0.325	4	3	33	10s
3	0.343	5	4	56	5imn
3	0.360	8	6	165	3h
4	0.372	7	5	126	59 min
4	0.385	6	4	210	10.3h

In simulation of extended multiple fault attack in Table 4, the bound of unknown part is closely related to the parameters t, k. Therefore, on the same number of faulty signatures, we use different parameters to compute the bound. For example, For the faulty signature number $\ell = 3$, the bound is 0.343 when selecting $t = 5, k = 4$, while it become 0.360 when choosing $t = 8, k = 6$. Both results are better than one in Table 3. But when $t = 4, k = 3$, the bound 0.325 is less than one in Table 3. The dimension of lattice increase very fast with the parameters t, k, so the extended attack is efficient in practice when ℓ is small.

5 Conclusion

The paper discusses an extended multiple fault attack against a probabilistic version of ISO/IEC 9796-2 with some particular parts of the unknown message. Instead of the general case, we only argue a case that some lower order bits of message are unknown which makes our attacks simpler. In the beginning, we use the method of solving simultaneous diophantine approximation problem to give a multiple fault attack. The dimension of lattice to be computed is the number of faulty signatures plus one. And then we apply the Cohn-Heninger technique to improve the bound, while the dimension of lattice is increased very fast with the signature number.

6 Acknowledgements

This work was supported by the National Natural Science Foundation of China (No.61133013) and the Tsinghua University Initiative Scientic Research Program (No.20111080970).

References

1. Boneh, D., DeMillo, R.A., Lipton, R.J.: On the Importance of Checking Cryptographic Protocols for Faults. Journal of Cryptology 14(2), 101-119 (2001)
2. Cohn, H., Heninger, N.: Approximate Common Divisiors Via Lattices. Cryptology ePrint Archive, Report 2011/437, http://eprint.iacr.org/2011/437.
3. Coppersmith, D.: Small Solutions to Polynomial Equations, and Low Exponent Vulnerabilities. Journal of Cryptology 10(4), 233-260 (1997)
4. Coron, J.-S., Joux, A., Kizhvatov, I., Naccache, D., Paillier, P.: Fault Attacks on RSA Signatures with Partially Unknown Messages. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 444-456. Springer, Heidelberg (2009). Full version: eprint.iacr.org/2009/309.

5. Coron, J.-S., Naccache, D., Stern, J.P.: On the Security of RSA Padding. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 1-18. Springer, Heidelberg (1999).
6. Coron, J.-S., Naccache, D., Tibouchi, M.: Fault Attacks Against EMV Signatures. In: Pieprzyk, J. (Ed.): CT-RSA 2010. LNCS vol. 5985, pp. 208-220, Springer, Heidelberg (2010)
7. Coron, J.-S., Naccache, D., Tibouchi, M., Weinmann, R.P.: Practical Cryptanalysis of ISO/IEC 9796-2 and EMV signatures. In: Halevi, S. (ed.) Advances in Cryptology-CRYPTO 2009. LNCS, vol. 5677, pp. 428-444. Springer, Heidelberg (2009)
8. Herrmann, M., May, A.: Solving Linear Equations Modulo Divisors: On Factoring Given Any Bits. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 406-424. Springer, Heidelberg (2008)
9. Howgrave-Graham, N.: Approximate integer common divisors. In: Silverman. J. H. (ed.) CALC 2001. LNCS, vol. 2146, pp. 51-66. Springer, Heidelberg (2001)
10. ISO/IEC 9796-2, Information TechnologyCSecurity Techniques-Digital Signature Schemes Giving Message Recovery-Part 2: Mechanisms Using a Hash-Funcion (1997)
11. ISO/IEC 9796-2: 2002 Information Technology Security Techniques-Digital Signature Schemes Giving Message Recovery-Part 2: Integer Factorization Based Mechanisms (2002)
12. Lenstra, A., Lenstra Jr., H., Lovász, L.: Factoring Polynomials with Rational Coefficients. Mathematische Annalen 261, 513-534 (1982)
13. Rivest, R., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Communications of the ACM, 120-126 (1978)
14. Shoup,V.: Number Theory C++ Library (NTL) version 5.5.2. www.shoup.net/ntl/