Cryptanalysis of Countermeasures Proposed for Repairing ISO 9796-1

Marc Girault and Jean-François Misarsky

France Télécom - CNET
42 rue des Coutures, B.P. 6243
14066 CAEN CEDEX 4, FRANCE
{marc.girault, jeanfrancois.misarsky}@cnet.francetelecom.fr

Abstract. ISO 9796-1, published in 1991, was the first standard specifying a digital signature scheme with message recovery. In [4], Coron, Naccache and Stern described an attack on a slight modification of ISO 9796-1. Then, Coppersmith, Halevi and Jutla turned it into an attack against the standard in full [2]. They also proposed five countermeasures for repairing it. In this paper, we show that all these countermeasures can be attacked, either by using already existing techniques (including a very recent one), or by introducing new techniques, one of them based on the decomposition of an integer into sums of two squares.

1 Introduction: ISO 9796-1 and Forgery

The first standard on digital signature scheme with message recovery is ISO 9796-1 [10]. At the end of 80's, no hash-function standard was available. Consequently, ISO 9796-1 used only redundancy function to resist attacks that exploit the multiplicative property of the RSA cryptosystem. The precautions taken in this standard are described in [8]. Until the *rump session* of Crypto '99, no known attack [13] was able to forge a signature complied with the ISO 9796-1 standard.

1.1 The ISO 9796-1 Standard

This standard specifies how a message m is encoded to a valid message $\mu_{iso}(m)$ before applying the RSA signature function. Only redundancy is used, no hash-function. Notations used in this paper to describe encoded functions are the same as in [2]:

- $s(x)$: the function mapping 4 bits of message to 4 bits of redundancy. It is an Hamming code (8, 8, 4).
- $\bar{s}(x)$: the result of setting the most significant bit of $s(x)$ to 1:

$$\bar{s}(x) = s(x) \text{ OR } 1000 \ . \tag{1}$$

- $\tilde{s}(x)$: the result of flipping the least significant bit of $s(x)$:

$$\tilde{s}(x) = s(x) \oplus 0001 \ . \tag{2}$$

When the length of the modulus is $16z+1$ bits and the length of the message is $8z+1$ bits, the encoding function, or redundancy function μ_{iso}, is defined as follows:

$$\begin{aligned}\mu_{iso}(m) = {} & \bar{s}(m_{l-1})\tilde{s}(m_{l-2})m_{l-1}m_{l-2} \\ & s(m_{l-3})s(m_{l-4})m_{l-3}m_{l-4} \\ & \ldots \\ & s(m_3)s(m_2)m_3m_2 \\ & s(m_1)s(m_0)m_0 6 \ .\end{aligned} \tag{3}$$

1.2 Attack Against a Slight Modification of ISO 9796-1

At first, a new strategy of forgery was presented at Crypto '99 by Coron, Naccache and Stern in their paper [4]. They described an attack against a slight modification of ISO 9796-1. Their forgery is possible when the length of the modulus is $16z+1$ bits, the length of the message is $8z+1$ bits, and the valid message $\mu(m)$ is defined as follows:

$$\begin{aligned}\mu(m) = {} & \bar{s}(m_{l-1})s(m_{l-2})m_{l-1}m_{l-2} \\ & s(m_{l-3})s(m_{l-4})m_{l-3}m_{l-4} \\ & \ldots \\ & s(m_3)s(m_2)m_3m_2 \\ & s(m_1)s(m_0)m_0 6 \ .\end{aligned} \tag{4}$$

Remark 1. $\mu(m) = \mu_{iso}(m)$ except that $\tilde{s}(m_{l-2})$ is replaced by $s(m_{l-2})$.

1.3 Attack Against ISO 9796-1 and Countermeasures

At the *rump session* of Crypto '99, Coppersmith, Halevi and Jutla described a modified version of the attack of Coron, Naccache and Stern to forge a signature of a chosen message when the encoding function μ_{iso} of ISO standard is used, i.e. (3). After Crypto conference, they submitted a contribution [2] to "IEEE P1363 research contributions". In their paper, they proposed five possible countermeasures to avoid forgeries. Their solutions avoid Coron-Naccache-Stern-like forgeries, but not all forgeries as we show now.

More precisely, we present various chosen messages attacks against all the five countermeasures, in which the signatures of two (or three) messages chosen by the enemy allow him to forge the signature of another one.

2 Massive Mask Changes

Coppersmith, Halevi and Jutla propose three solutions based on the massive mask change technique. In their propositions, they use the same principle of dispersion as in ISO 9796-1.

Remark 2. These three propositions allow message recovery, but nothing notifies the length of the message. In ISO 9796-1 [10], a nibble was modified in order to mark the length of the message.

2.1 μ_1: Fixed Redundancy

In the first proposition, μ_1, only fixed redundancy is used. The i'th nibble, π_i in the hexadecimal expansion of the irrational number $\pi = 3.14159...$, is used to obtain redundancy. Note that the number of bits of redundancy is half the number of bits of the RSA modulus n.

$$\begin{aligned}\mu_1(m) = \; & \pi_{l-1}\pi_{l-2}m_{l-1}m_{l-2} \\ & \pi_{l-3}\pi_{l-4}m_{l-3}m_{l-4} \\ & \dots \\ & \pi_1\pi_0 m_1 m_0 \;\; .\end{aligned} \tag{5}$$

The Coron-Naccache-Stern-like forgeries are avoided. But we are at the limit of the efficiency of the forgery described in [12], which allows to find three messages m_1, m_2, m_3 such that $\mu_1(m_1)\mu_1(m_2) = \mu_1(m_3) \pmod{n}$ and therefore, given signatures of m_1 and m_2, forge the signature of m_3. Moreover, the limit of this attack is heuristic. Consequently, the forgery in [12] may be used.

2.2 μ_2 and μ_3: Irrational Numbers and Exclusive-OR

With μ_2 and μ_3, the attacks based on the Coron-Naccache-Stern forgery [4], [2], are also avoided. In these cases, the i'th nibbles, π_i and e_i in the hexadecimal expansion of the irrational numbers $\pi = 3.14159...$ and $e = 2.71828...$ respectively, are used. Moreover, the native redundancy of ISO 9796-1 is present and plays its role to defeat the other forgeries [13].

$$\begin{aligned}\mu_2(m) = \; & (\pi_{l-1} \oplus s(m_{l-1}))(\pi_{l-2} \oplus s(m_{l-2}))m_{l-1}m_{l-2} \\ & (\pi_{l-3} \oplus s(m_{l-3}))(\pi_{l-4} \oplus s(m_{l-4}))m_{l-3}m_{l-4} \\ & \dots \\ & (\pi_1 \oplus s(m_1))(\pi_0 \oplus s(m_0))m_1 m_0 \;\; .\end{aligned} \tag{6}$$

$$\begin{aligned}\mu_3(m) = \; & (\pi_{l-1} \oplus s(m_{l-1} \oplus e_{l-1}))(\pi_{l-2} \oplus s(m_{l-2} \oplus e_{l-2}))m_{l-1}m_{l-2} \\ & (\pi_{l-3} \oplus s(m_{l-3} \oplus e_{l-3}))(\pi_{l-4} \oplus s(m_{l-4} \oplus e_{l-4}))m_{l-3}m_{l-4} \\ & \dots \\ & (\pi_1 \oplus s(m_1 \oplus e_1))(\pi_0 \oplus s(m_0 \oplus e_0))m_1 m_0 \;\; .\end{aligned} \tag{7}$$

Nevertheless, a new attack by Grieu [6], disclosed in October 1999, can be applied to these functions of redundancy. This attack is originally against the ISO 9796-1 [10], but the principle of this attack can be used to forge a signature when μ_2 or μ_3 is the redundancy function in a signature scheme. This forgery is based on the multiplicative property of the RSA cryptosystem and, for any public exponent, the forged signature of a message is obtained from the signature of three other messages. This attack is computationally inexpensive and works for modulus of $16z$, $16z \pm 1$, or $16z \pm 2$ bits.

3 Length Expanding Encoding: μ_4

The encoded function μ_4 involves encoding the message m into a string longer than the modulus n. This solution does not have the property of message recovery. Two constants c_0 and c_1 are fixed, each half the length of the modulus n. The message m is also half the length of the modulus. The redundancy function μ_4 is defined[1] as follows :

$$\mu_4(m) = (m + c_0)||(m + c_1)||m \ . \tag{8}$$

We can easily write μ_4 as an affine function:

$$\begin{aligned}\mu_4(m) &= (m + c_0)||(m + c_1)||m \\ &= (m + c_0)2^\alpha + (m + c_1)2^\beta + m \\ &= m\underbrace{(2^\alpha + 2^\beta + 1)}_{\omega} + \underbrace{c_0 2^\alpha + c_1 2^\beta}_{a} \\ &= m\omega + a \ .\end{aligned} \tag{9}$$

We are at the limit of the efficiency of the forgery described in [5] against signature scheme with an affine function of redundancy. This forgery allows to find three messages m_1, m_2, m_3 such that $\mu_4(m_1)\mu_4(m_2) = \mu_4(m_3) \pmod n$ and therefore, given signatures of m_1 and m_2, forge the signature of m_3. Moreover, the limit of this attack is heuristic. Consequently, the forgery in [5] may be used.

4 Encoding via Squaring: μ_5

The redundancy function μ_5 is defined as follows :

$$\mu_5(m) = m^2 + \delta \ . \tag{10}$$

where δ is a fixed random constant of about the same size as the RSA modulus n and the message m is less than the square root of the modulus n. We present two forgeries when μ_5 is used.

First forgery[2]**:** Forges the signature of the message $(m_1 m_2 + \delta \pmod n)$ with the signatures of m_1 and m_2 such that:

$$m_2 = m_1 + 1 \ . \tag{11}$$

Second forgery: Forges the signature of a message in the set $\{x, y, z, t\}$ when we can write $A = 2(n - \delta)$ as at least two different sums of two squares:

$$A = x^2 + y^2 = z^2 + t^2 \quad (x, y) \neq (z, t) \text{ and } (y, x) \neq (z, t) \ . \tag{12}$$

[1] The symbol || denotes the concatenation of two strings.

[2] Discovered independently by D. Naccache.

4.1 First Forgery

Let m_1 and m_2 be two messages such that :

$$m_2 = m_1 + 1 \ . \tag{13}$$

Then we have :

$$\begin{aligned}
\mu_5(m_1)\mu_5(m_2) &= (m_1^2+\delta)(m_2^2+\delta) \\
&= (m_1 m_2)^2 + \delta(m_1^2+m_2^2) + \delta^2 \\
&= (m_1 m_2+\delta)^2 - 2m_1 m_2\delta + \delta(m_1^2+m_2^2) \\
&= (m_1 m_2+\delta)^2 + \delta(m_1^2 - 2m_1 m_2 + m_2^2) \\
&= (m_1 m_2+\delta)^2 + \delta\underbrace{(m_1-m_2)^2}_{1} \\
&= \mu_5(m_1 m_2+\delta) \\
&= \mu_5(m_1 m_2+\delta \ (\mathrm{mod}\, n)) \pmod n \ .
\end{aligned} \tag{14}$$

Now, we can find m_1 and m_2 s.t. $m_1 m_2 + \delta \pmod n$ is less than $\sqrt{n}$ by choosing m_1 close enough to $\sqrt{n-\delta}$. More precisely, let $m_1 = \sqrt{n-\delta} + \theta$ such that $\theta \in \left[-\frac{1}{2}, \frac{1}{2}\right]$. Then :

$$\begin{aligned}
m_1 m_2 + \delta &= m_1(m_1+1) + \delta \\
&= m_1^2 + m_1 + \delta \\
&= (\sqrt{n-\delta}+\theta)^2 + (\sqrt{n-\delta}+\theta) + \delta \\
&= (2\theta+1)\sqrt{n-\delta} + \theta(\theta+1) \pmod n \ .
\end{aligned} \tag{15}$$

and will be certainly (resp. possibly) smaller than $\sqrt{n}$ if $\theta \in \left[-\frac{1}{2}, 0\right]$ (resp. if $\theta \in \left]0, \frac{1}{2}\right]$). Of course, other values of m_1 and m_2 can be suitable, depending on the value of $\sqrt{n-\delta}$. Moreover, one can choose a large value for θ as long as $m_1 m_2 + \delta \pmod n$ is less than $\sqrt{n}$.

4.2 Second Forgery

The second forgery uses the fact that many integers can be written as sums of two squares in (at least) two different ways. This will be applied to various values of $A = 2(n-\delta)$, where n is a RSA modulus. Roughly speaking, if we can write:

$$A = x^2 + y^2 = z^2 + t^2, \quad (x,y) \text{ and } (y,x) \neq (z,t) \ . \tag{16}$$

then it comes (see (25)):

$$\mu_5(x)\mu_5(z) = \mu_5(y)\mu_5(t) \pmod n \ . \tag{17}$$

and the signature of any message in the set $\{x,\, y,\, z,\, t\}$ can be deduced from the signatures of the three other ones. To do that, we first need to recall some basic results from (computational) number theory.

The sum of two squares in two ways. In 17^{th} century, Fermat proved that every prime p such that $p = 1 \pmod 4$ has a unique decomposition as a sum of two squares and, more generally, that an integer n has such a decomposition if and only if all its prime factors such that $p = 3 \pmod 4$ have even exponents in the factorization of n. In the latter case, the number of essentially different decompositions[3] is 2^{k-1}, where k is the number of primes such that $p = 1$ (mod 4) [9]. Here, we will be specially interested in the case $k \geq 2$.

Remark 3. (Gauss) If a number n can be written as a sum of squares then n has $\left\lceil \frac{\prod_i (e_i+1)}{2} \right\rceil$ representations[4] [7, section 182] where the e_i are the powers of the prime factors p_i of n such that $p_i = 1 \pmod 4$.

Diophante's identities are crucial in the proof of these theorems. We recall them:

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= (ac-bd)^2+(bc+ad)^2 = e_1^2+f_1^2 \\ &= (ac+bd)^2+(bc-ad)^2 = e_2^2+f_2^2 \ .\end{aligned} \tag{18}$$

They show that the product of two sums of two squares is still the sum of two squares, and in two different ways (see example 1). There is an exception to the latter statement: if one of the initial sums is equal to 2 ($= 1^2 + 1^2$), then the two identities become only one, and the decomposition remains the same (see example 2).

Example 1.

$$\begin{aligned}13.17 &= (2^2+3^2)(4^2+1^2) \\ &= (2.4-3.1)^2+(3.4+2.1)^2 = 5^2+14^2 \\ &= (2.4+3.1)^2+(3.4-2.1)^2 = 11^2+10^2 \ .\end{aligned} \tag{19}$$

Example 2.

$$\begin{aligned}2.13 &= (1^2+1^2)(2^2+3^2) \\ &= (1.2-1.3)^2+(1.2+1.3)^2 = \ 1^2+5^2 \\ &= (1.2+1.3)^2+(1.2-1.3)^2 = 5^2+1^2 \ .\end{aligned} \tag{20}$$

Now, the point is to make, when existing, these decompositions efficient. In 1908, Cornacchia [3] showed how to use Euclid's algorithm to find the decomposition of a prime p equal to 1 modulo 4 [1, pages 34-35], [15]. It can be briefly described as follows: find a square root z of -1 modulo p, then apply Euclid's algorithm to p and z, until the remainder x is smaller than $\sqrt{p}$. Then it can be proven that $p - x^2$ is a square y^2 and we have: $p = x^2 + y^2$.

Finally, it is trivial to remark that the product of a square and of a sum of two squares is still a sum of two squares:

$$C^2(x^2+y^2) = (Cx)^2 + (Cy)^2 \ . \tag{21}$$

[3] $n = a^2 + b^2$ with $\gcd(a, b) = 1$ and $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$.

[4] $n = a^2 + b^2$ with $(a, b) \in \mathbb{N} \times \mathbb{N}$.

As a consequence of all these facts, if we can write $A = 2(n-\delta)$ as a product in the form:

$$C^2 \prod_{i=1}^{k} p_i \quad \text{or} \quad 2C^2 \prod_{i=1}^{k} p_i \quad . \tag{22}$$

where the p_i are equal to 1 modulo 4 and $k \geq 2$, then, by applying Cornacchia's algorithm to the p_i and applying Diophante's identities to its outputs, we will obtain at least 2^{k-1} different decompositions of A in sums of two squares.

Example 3. $n = 493 = 17.29$ and $\delta = 272$.
Then $A = 2(n-\delta) = 2.13.17$.
We have $13 = 2^2 + 3^2$, $17 = 4^2 + 1^2$.
And, by applying Diophante's identities:

$$\begin{aligned} A = 2(5^2 + 14^2) &= (1^2 + 1^2)(5^2 + 14^2) &= 9^2 + 19^2 \\ = 2(11^2 + 10^2) &= (1^2 + 1^2)(11^2 + 10^2) &= 1^2 + 21^2 \quad . \end{aligned} \tag{23}$$

If we cannot write A as such a product, either because its factorization reveals a prime equal to 3 mod 4 with an odd exponent, or reveals only one prime equal to 1 modulo 4, or simply because we failed in factorizing $n - \delta$, then we have to try again with another value of n. This leads to the following forgery method.

Forgery.

Step 1: Try different moduli n until obtaining:

$$\begin{aligned} A &= x^2 + y^2 & x,\, y,\, z,\, t < \sqrt{n} \\ &= z^2 + t^2 & (x,\, y) \neq (z,\, t) \text{ and } (y,\, x) \neq (z,\, t) \quad . \end{aligned} \tag{24}$$

Step 2: Obtain the signature of 3 messages in the set $\{x, y, z, t\}$.
Step 3: Use the following relation to compute the signature of the remaining message:

$$\begin{aligned} \mu_5(x)\mu_5(z) &= (x^2 + \delta)(z^2 + \delta) \\ &= (A - y^2 + \delta)(A - t^2 + \delta) \\ &= (-y^2 - \delta)(-t^2 - \delta) \\ &= (y^2 + \delta)(t^2 + \delta) \\ &= \mu_5(y)\mu_5(t) \qquad \pmod{n} \quad . \end{aligned} \tag{25}$$

Example 4. $n = 493 = 17.29$ and $\delta = 272$.
Then $A = 9^2 + 19^2 = 1^2 + 21^2$ (see example 3).

$$\begin{aligned} \mu_5(9)\mu_5(1) &= (9^2 + 272)(1^2 + 272) \\ &= 234 \qquad \pmod{493} \quad . \end{aligned} \tag{26}$$

And,

$$\begin{aligned} \mu_5(19)\mu_5(21) &= (19^2 + 272)(21^2 + 272) \\ &= 234 \qquad \pmod{493} \quad . \end{aligned} \tag{27}$$

Remark 4. The attack can be extended to $A = 3n - 2\delta$, if $\delta > \frac{n}{2}$ (if not, A will be too large and some elements in the set $\{x,\, y,\, z,\, t\}$ will be greater than $\sqrt{n}$).

Example 5. We try our attack on the signature scheme where the RSA-modulus is the modulus specified in the Annex A of ISO 9796-1 [10]. All values in this example are in hexadecimal.

$$\begin{aligned} p = \quad & \texttt{BA09106C 754EB6FE BBC21479 9FF1B8DE} \\ & \texttt{1B4CBB7A 7A782B15 7C1BC152 90A1A3AB} \end{aligned} \tag{28}$$

$$\begin{aligned} q = \quad & \texttt{1 6046EB39 E03BEAB6 21D03C08 B8AE6B66} \\ & \texttt{CFF955B6 4B4F48B7 EE152A32 6BF8CB25} \end{aligned} \tag{29}$$

$$\begin{aligned} n = \quad & \texttt{1 00000000 00000000 00000000 00000000} \\ & \texttt{BBA2D15D BB303C8A 21C5EBBC BAE52B71} \\ & \texttt{25087920 DD7CDF35 8EA119FD 66FB0640} \\ & \texttt{12EC8CE6 92F0A0B8 E8321B04 1ACD40B7} \end{aligned} \tag{30}$$

Let δ a random constant of about the same size as the modulus n:

$$\begin{aligned} \delta = \quad & \texttt{FFE3B564 A0CB8C6C 6585C9CF A1CFC64B} \\ & \texttt{64B0C0F9 6CE980F5 ACC276C1 13045D1D} \\ & \texttt{05B1D218 D58C7D32 2387A305 9547EC31} \\ & \texttt{CF62CA5D 8C316E99 24B7F2C1 8A873FAE} \end{aligned} \tag{31}$$

Compute the factorization of A:

$$\begin{aligned} A &= 2(n - \delta) \\ &= \texttt{2.2F9.2F9D10D.} \\ &\quad \texttt{200000011}^{2}\texttt{.3FE9820B7AE6D}^{5}\texttt{.} \\ &\quad \texttt{3385F065A24DB4467E066FBBD577A0C6F6D119} \end{aligned} \tag{32}$$

With the Cornacchia algorithm and by applying the Diophante's identities we obtain 72 couples of values $(a_i,\, b_i)$ such that $a_i^2 + b_i^2 = A$. And all these values are less than $\sqrt{n}$. We give 4 couples as examples:

$$\begin{aligned} a_1 &= \texttt{10F26AC8 379A5197 8F6D6E3E 17461ED9} \\ &\quad\, \texttt{1642DE79 C90D14D5 923190C6 D0A0EB} \\ b_1 &= \texttt{78599149 C677F865 48F58E83 DA99C194} \\ &\quad\, \texttt{9F653DBD FAEA8B8C 02BCDD8D 04F7F5B} \end{aligned} \tag{33}$$

$$\begin{aligned} a_2 &= \texttt{15CCECF3 6BC80743 296A7F88 78FFC0E2} \\ &\quad\, \texttt{D509B3C9 B1EA0B53 8FE5036E B23E93} \\ b_2 &= \texttt{7858C944 CDCA3E18 0B0477F2 C6728C54} \\ &\quad\, \texttt{BC4ADCD1 17361A46 2C0D7267 8661173} \end{aligned} \tag{34}$$

$$\begin{aligned} a_3 &= \texttt{274AEA5B 8289F65F 2C849CA7 DA69F691} \\ &\quad\, \texttt{15430C53 4EA3101F ACF6B8A8 673DDF} \\ b_3 &= \texttt{78545894 164142A8 FC5E800A 3DAC3705} \\ &\quad\, \texttt{BBAD4B7C 46AE5A24 1B4D5830 E9FC137} \end{aligned} \tag{35}$$

$$\begin{aligned} a_4 &= \texttt{4CE8CD96 B9920AB2 075E197C 564950E1} \\ &\quad\ \texttt{18BA416D 9FEC2BDF 5BE6BBEF C18F45} \\ b_4 &= \texttt{78422D6B ED414DAD 9BE47D08 F2CF8EF8} \\ &\quad\ \texttt{D742C8E5 C0440C45 F2B3300E B3E4A75} \end{aligned} \tag{36}$$

5 Conclusion

We have shown that all the countermeasures described in "ISO 9796 and the new forgery strategy (Working Draft)" [2] by Coppersmith, Halevi and Jutla can be attacked. For two propositions, we use previous forgeries presented at Eurocrypt '97 and Crypto '97. For the propositions two and three, μ_2 and μ_3, a recent attack is used. Moreover, we present two new ways to forge a signature when the last proposition is used.

Our contribution on the cryptanalysis of signature schemes with redundancy, after De Jonge-Chaum [11], Girault-Misarsky [5], Misarsky [12], Coron-Naccache-Stern [4] and Coppersmith-Halevi-Jutla [2] shows that is very difficult to define this kind of scheme. But, perhaps it is a good challenge for a year with a high level of redundancy (three zeroes) such as the year 2000.

6 Acknowledgements

We are grateful to Jean-Louis Nicolas for pointing out Cornacchia's algorithm to us and to Yves Hellegouarch for results picked out from his nice *Invitation aux mathématiques de Fermat-Wiles* [9].

References

1. Cohen, H.: A Course in Computational Algebraic Number Theory. Graduate Texts in Mathematics **138** Springer-Verlag (1995)
2. Coppersmith, D., Halevi, S., Jutla, C.: ISO 9796-1 and the new forgery strategy (Working Draft). Research Contribution to P1363 (1999) http://grouper.ieee.org/groups/1363/contrib.html
3. Cornacchia, G.: Su di un metodo per la risoluzione in numeri unteri dell' equazione $\sum_{h=0}^{n} C_h x^{n-h} y^h = P$. Giornale di Matematiche di Battaglini **46** (1908) 33–90
4. Coron, J.-S., Naccache, D., Stern, J. P.: On the Security of RSA Padding. Advances in Cryptology - Crypto '99 - Lecture Notes in Computer Science **1666** Springer-Verlag (1999) 1–18
5. Girault, M., Misarsky, J.-F.: Selective Forgery of RSA Signatures Using Redundancy. Advances in Cryptology - Eurocrypt '97 - Lecture Notes in Computer Science **1233** Springer-Verlag (1997) 495–507
6. Grieu, F.: A Chosen Messages Attack on ISO/IEC 9796-1 Signature Scheme. Advances in Cryptology - Eurocrypt 2000 - Lecture Notes in Computer Science **1807** Springer-Verlag (2000) **??**–**??** (this volume)
7. Gauss, C.F.: Disquisitiones Arithmeticae. Reissue Edition Springer-Verlag (1986)

8. Guillou, L.C., Quisquater, J.J., Walker, M., Landrock, P., Shaer, C.: Precautions Taken Against Various Potential Attacks in ISO/IEC DIS 9796, Digital Signature Scheme Giving Message Recovery. Advances in Cryptology - Eurocrypt '90 - Lecture Notes in Computer Science **473** Springer-Verlag (1991) 465–473
9. Hellegouarch, Y.: Invitation aux Mathématiques de Fermat-Wiles. Masson (1997)
10. ISO: ISO/IEC 9796-1, Information technology – Security techniques – Digital signature schemes giving message recovery – Part 1: Mechanisms using redundancy. (1991)
11. De Jonge, W., Chaum, D.: Attacks on Some RSA Signatures. Advances in Cryptology - Crypto '85 - Lecture Notes in Computer Science **218** Springer-Verlag (1986) 18–27
12. Misarsky, J.-F.: A Multiplicative Attack using LLL Algorithm on RSA Signatures with Redundancy. Advances in Cryptology - Crypto '97 - Lecture Notes in Computer Science **1294** Springer-Verlag (1997) 221–234
13. Misarsky, J.-F.: How (not) to Design RSA Signature Schemes. Public Key Cryptography - First International Workshop on Pratice and Theory in Public Key Cryptography - PKC'98 Lecture Notes in Computer Science **1431** Springer-Verlag (1998) 14–28
14. Morain, F.: Courbes elliptiques et tests de primalité. Thesis (1990)
15. Morain, F., Nicolas, J.-L.: On Cornacchia's algorithm for solving the diophantine equation $u^2 + dv^2 = m$. Chapter 2 of [14]
ftp://ftp.inria.fr/INRIA/publication/Theses/TU-0144/ch2.ps