Cryptanalysis of RSA Signatures with Fixed-Pattern Padding

Eric Brier[1], Christophe Clavier[1], Jean-Sébastien Coron[2], and David Naccache[2]

[1] Gemplus Card International
Parc d'Activités de Gémenos, B.P. 100, 13881 Gémenos Cedex, France
{eric.brier, christophe.clavier}@gemplus.com
[2] Gemplus Card International
34 rue Guynemer, 92447 Issy-les-Moulineaux, France
{jean-sebastien.coron, david.naccache}@gemplus.com

Abstract. A fixed-pattern padding consists in concatenating to the message m a fixed pattern P. The RSA signature is then obtained by computing $(P|m)^d \bmod N$ where d is the private exponent and N the modulus. In Eurocrypt '97, Girault and Misarsky showed that the size of P must be at least half the size of N (in other words the parameter configurations $|P| < |N|/2$ are insecure) but the security of RSA fixed-pattern padding remained unknown for $|P| > |N|/2$. In this paper we show that the size of P must be at least two-thirds of the size of N, *i.e.* we show that $|P| < 2|N|/3$ is insecure.

Key-words: RSA signatures, fixed-pattern padding, affine redundancy.

1 Introduction

RSA was invented in 1977 by Rivest, Shamir and Adleman [8], and is now the most widely used public-key cryptosytem. RSA is commonly used for providing privacy and authenticity of digital data, and securing web traffic between servers and browsers.

A very common practice for signing with RSA is to first hash the message, add some padding, and then raise the result to the power of the decryption exponent. This paradigm is the basis of numerous standards such as PKCS #1 v2.0 [9].

In this paper, we consider RSA signatures with fixed-pattern padding, without using a hash function. To sign a message m, the signer concatenates a fixed padding P to the message, and the signature is obtained by computing:

$$s = (P|m)^d \bmod N$$

where d is the private exponent and N the modulus.

More generally, we consider RSA signatures in which a simple affine redundancy is used. To sign a message m, the signer first computes:

$$R(m) = \omega \cdot m + a \quad \text{where} \begin{cases} w \text{ is the multiplicative redundancy} \\ a \text{ is the additive redundancy} \end{cases} \tag{1}$$

The signature of m is then:

$$s = R(m)^d \bmod N$$

A left-padded redundancy scheme $P|m$ is obtained by taking $\omega = 1$ and $a = P \cdot 2^\ell$, whereas a right-padding redundancy scheme $m|P$ is obtained by taking $\omega = 2^\ell$ and $a = P$.

No proof of security is known for RSA signatures with affine redundancy, and several attacks on such formats have appeared (see [6] for a thorough survey). At Crypto '85, De Jonge and Chaum [1] exhibited a multiplicative attack against RSA signatures with affine

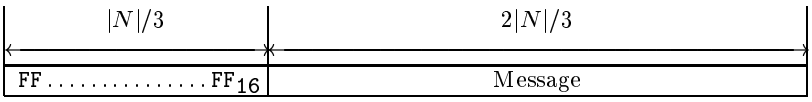

Fig. 1. Example of an RSA padding forgeable by De Jonge and Chaum's method where $\omega = 1$ and $a =$ $\texttt{FF...FF 00...00}_{16}$

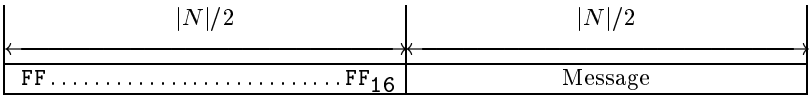

Fig. 2. Example of an RSA padding forgeable by Girault and Misarsky's method where $\omega = 1$ and $a =$ $\texttt{FF...FF 00...00}_{16}$

redundancy, based on the extended Euclidean algorithm. Their attack applies when the multiplicative redundancy ω is equal to one and the size of the message is at least two-thirds of the size of the RSA modulus N.

$$|\text{message}| \succ \frac{2}{3}|N|$$

For example, a signature can be forged if one uses the affine redundancy of figure 1.

De Jonge and Chaum's attack was extended by Girault and Misarsky [2] at Eurocrypt '97, using Okamoto-Shiraishi's algorithm [7], which is an extension of the extended Euclidean algorithm. They increased the field of application of multiplicative attacks on RSA signatures with affine redundancy as their attack applies to any value of ω and a, when the size of the message is at least half the size of the modulus (refer to figure 2 for an illustration):

$$|\text{message}| \succ \frac{1}{2}|N|$$

Girault and Misarsky also extended the multiplicative attacks to RSA signatures with modular redundancy:

$$R(m) = \omega_1 \cdot m + \omega_2 \cdot (m \bmod b) + a \quad \text{where} \begin{cases} w_1, w_2 & \text{is the multiplicative redundancy} \\ a & \text{is the additive redundancy} \\ b & \text{is the modular redundancy} \end{cases} \tag{2}$$

In this case, the size of the message must be at least half the size of the modulus plus the size of the modular redundancy.

Finally, Girault and Misarsky's attack was extended by Misarsky [5] at Crypto '97 to a redundancy function in which the message m and the modular redundancy $m \bmod b$ can be split into different parts, using the LLL algorithm [4]. The attack applies when the size of the message is at least half the size of the modulus plus the size of the modular redundancy.

In this paper, we extend Girault and Misarsky's attack against RSA signatures with affine redundancy to messages of size as small as one third of the size of the modulus, as illustrated in figure 3.

$$|\text{message}| \succ \frac{1}{3}|N|$$

As Girault and Misarsky's attack, our attack applies for any w and a and runs in polynomial time. However, our attack is existential only, as we cannot choose the message the signature of which we forge, whereas Girault and Misarsky's attack is selective: they can choose the message which signature is forged.

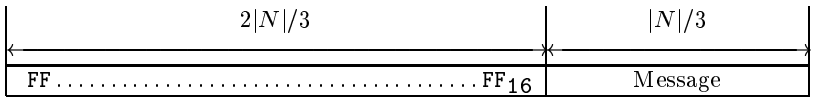

Fig. 3. Example of an RSA padding forgeable by our technique where the ω is equal to one and $a =$ FF...FF 00...00$_{16}$

2 The new attack

In this section we extend Girault and Misarsky's multiplicative attack on RSA signatures with affine redundancy, to messages of size as small as one third of the size of N. A multiplicative attack is an attack in which the redundancy function of a message can be expressed as a multiplicative combination of the redundancy functions of other messages. So we look for four distinct messages m_1, m_2, m_3 and m_4, each as small as one third of the size of the modulus, such that:

$$R(m_1) \cdot R(m_2) = R(m_3) \cdot R(m_4) \bmod N \tag{3}$$

Then, using the signatures of m_2, m_3 and m_4, one can forge the signature of m_1 by:

$$R(m_1)^d = \frac{R(m_3)^d \cdot R(m_4)^d}{R(m_2)^d} \bmod N$$

From (3) we obtain:

$$(\omega \cdot m_1 + a) \cdot (\omega \cdot m_2 + a) = (\omega \cdot m_3 + a) \cdot (\omega \cdot m_4 + a) \bmod N$$

Denoting $P = a/\omega \bmod N$, we obtain:

$$(P + m_1) \cdot (P + m_2) = (P + m_3) \cdot (P + m_4) \bmod N$$

and letting:

$$\begin{array}{ll} t = m_3 & y = m_2 - m_3 \\ x = m_1 - m_3 & z = m_4 - m_1 - m_2 + m_3 \end{array} \tag{4}$$

we obtain:

$$((P + t) + x) \cdot ((P + t) + y) = (P + t) \cdot ((P + t) + x + y + z) \bmod N$$

which simplifies into:

$$x \cdot y = (P + t) \cdot z \bmod N \tag{5}$$

Our goal is consequently to find four integers x, y, z and t, each as small as one third of the size of N, satisfying equation (5).

First, we obtain two integers z and u such that

$$P \cdot z = u \bmod N \quad \text{with} \quad \begin{cases} -N^{\frac{1}{3}} < z < N^{\frac{1}{3}} \\ 0 < u < 2 \cdot N^{\frac{2}{3}} \end{cases}$$

As noted in [3], this is equivalent to finding a good approximation of the fraction P/N, and can be done efficiently by developing it in continued fractions, *i.e.* applying the extended Euclidean algorithm to P and N. A solution is found such that $|z| < Z$ and $0 < u < U$ if $Z \cdot U > N$, which is the case here with $Z = N^{\frac{1}{3}}$ and $U = 2 \cdot N^{\frac{2}{3}}$.

We then select an integer y such that $N^{\frac{1}{3}} \leq y \leq 2 \cdot N^{\frac{1}{3}}$ and $\gcd(y, z) = 1$. We find the non-negative integer $t < y$ such that:

$$t \cdot z = -u \bmod y$$

which is possible since $\gcd(y, z) = 1$. Then we take

$$x = \frac{u + t \cdot z}{y} \leq 4N^{\frac{1}{3}}$$

and obtain:

$$P \cdot z = u = x \cdot y - t \cdot z \bmod N$$

which gives equation (5), with x, y, z and t being all smaller than $4 \cdot N^{\frac{1}{3}}$. From x, y, z, t we derive using (4) four messages m_1, m_2, m_3 and m_4, each of size one third the size of N:

$$\begin{array}{ll} m_1 = x + t & m_2 = y + t \\ m_3 = t & m_4 = x + y + z + t \end{array} \tag{6}$$

Since $-N^{1/3} < z < N^{1/3}$ and $y \geq N^{1/3}$, we have $y + z > 0$, which gives using $u \geq 0$:

$$x + t = \frac{u + t \cdot (y + z)}{y} \geq 0$$

which shows that the four integers m_1, m_2, m_3 and m_3 are non-negative, and we have

$$R(m_1) \cdot R(m_2) = R(m_3) \cdot R(m_4) \bmod N$$

The complexity of our attack is polynomial in the size of N. In appendix we give an example of such a forgery computed using RSA Laboratories' official 1024-bits challenge-modulus RSA-309.

3 Extension to selective forgery

The attack of the previous section is only existential: we can not choose the message to be forged. In this section we show how we can make the forgery selective, but in this case the attack is no longer polynomial. Let m_3 be the message which signature must be forged. Letting x, y, z and t as in (4), we compute two integers z and u such that

$$(P + t) \cdot z = u \bmod N \quad \text{with} \begin{cases} -N^{\frac{1}{3}} < z < N^{\frac{1}{3}} \\ 0 < u < 2 \cdot N^{\frac{2}{3}} \end{cases}$$

We then factor u, and try to write u as the product $x \cdot y$ of two integers of roughly the same size, so that eventually we have four integers x, y, z, t of size roughly one third of the size of the modulus, with:

$$x \cdot y = (P + t) \cdot z \bmod N$$

which gives

$$R(m_1) \cdot R(m_2) = R(m_3) \cdot R(m_4) \bmod N$$

The signature of m_3 can now be forged using the signatures of m_1, m_2 and m_4. For a 512-bit modulus the selective forgery attack is truly practical. For a 1024-bit modulus the attack is more demanding but still feasible.

4 Conclusion

We have extended Girault and Misarsky's attack on RSA signatures with affine redundancy: we described a chosen message attack against RSA signatures with affine redundancy for messages as small as one third of the size of the modulus. Consequently, when using a fixed padding $P|m$ or $m|P$, the size of P must be at least two-thirds of the size of N. Our attack is polynomial in the length of the modulus. It remains an open problem to extend this attack to even smaller messages (or, equivalently, to bigger fixed-pattern constants): we do not know if there exists a polynomial time attack against RSA signatures with affine redundancy for messages shorter than one third of the size of the modulus. However, we think that exploring to what extent affine padding is malleable increases our understanding of RSA's properties and limitations.

Acknowledgements. We would like to thank Christophe Tymen, Pascal Paillier, Helena Handschuh and Alexey Kirichenko for helpful discussions and the anonymous referees for their constructive comments.

References

1. W. De Jonge and D. Chaum, *Attacks on some RSA signatures*. Proceedings of Crypto '85, LNCS vol. 218, Springer-Verlag, 1986, pp. 18-27.
2. M. Girault and J.-F. Misarksy, *Selective forgery of RSA signatures using redundancy*, Proceedings of Eurocrypt '97, LNCS vol. 1233, Springer-Verlag, 1997, pp. 495–507.
3. M. Girault, P. Toffin and B. Vallée, *Computation of approximation L-th roots modulo n and application to cryptography*, Proceedings of Crypto '88, LNCS vol. 403, Springer-Verlag, 1988, pp. 100–117.
4. A. K. Lenstra, H.W. Lenstra and L. Lovász, *Factoring polynomials with rational coefficients*, Mathematische Annalen, vol. 261, n. 4, 1982, pp. 515–534.
5. J.-F. Misarsky, *A multiplicative attack using LLL algorithm on RSA signatures with redundancy*, Proceedings of Crypto '97, LNCS vol. 1294, Springer-Verlag, pp. 221–234.
6. J.-F. Misarsky, *How (not) to design RSA signature schemes*, Public-key cryptography, Springer-Verlag, Lectures notes in computer science 1431, pp. 14–28, 1998.
7. T. Okamoto and A. Shiraishi, *A fast signature scheme based on quadratic inequalities*, Proc. of the 1985 Symposium on Security and Privacy, April 1985, Oakland, CA.
8. R. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public key cryptosystems*, CACM 21, 1978.
9. RSA Laboratories, PKCS #1 : *RSA cryptography specifications*, version 2.0, September 1998.

A A practical forgery

We describe a practical forgery with $\omega = 1$ and $a = 2^{1023} - 2^{352}$, the modulus N being RSA Laboratories offical challenge RSA-309, which factorisation is still unknown.

$$
\begin{aligned}
N &= \text{RSA-309} \\
&= \texttt{bdd14965 645e9e42 e7f658c6 fc3e4c73 c69dc246 451c714e b182305b 0fd6ed47} \\
&\quad \texttt{d84bc9a6 10172fb5 6dae2f89 fa40e7c9 521ec3f9 7ea12ff7 c3248181 ceba33b5} \\
&\quad \texttt{5212378b 579ae662 7bcc0821 30955234 e5b26a3e 425bc125 4326173d 5f4e25a6} \\
&\quad \texttt{d2e172fe 62d81ced 2c9f362b 982f3065 0881ce46 b7d52f14 885eecf9 03076ca5}
\end{aligned}
$$

$$
\begin{aligned}
R(m_1) = {} & \texttt{7fffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff} \\
& \texttt{ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff} \\
& \texttt{ffffffff ffffffff ffffffff ffffffff ffffffff 00415df4 ca4219b6 ea5fa8e4} \\
& \texttt{e2eabcfc 61348b80 e7ccbac7 3d1f5cc7 249e1519 9412886a f76220c6 d1409cd6}
\end{aligned}
$$

$$
\begin{aligned}
R(m_2) = {} & \texttt{7fffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff} \\
& \texttt{ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff} \\
& \texttt{ffffffff ffffffff ffffffff ffffffff ffffffff 00127f44 f753253a a0348be7} \\
& \texttt{826e893f 693032db c2194dbb 3b81e1c2 630b66d3 1448a3f4 7fd2d34f b28aefd6}
\end{aligned}
$$

$$
\begin{aligned}
R(m_3) = {} & \texttt{7fffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff} \\
& \texttt{ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff} \\
& \texttt{ffffffff ffffffff ffffffff ffffffff ffffffff 00781bd4 e0c918a7 308fcff7} \\
& \texttt{8f64044c a35b4937 36cd37d7 93f281b5 fdd0a951 52a0479b 57dd73b2 25b6df85}
\end{aligned}
$$

$$
\begin{aligned}
R(m_4) = {} & \texttt{7fffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff} \\
& \texttt{ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff} \\
& \texttt{ffffffff ffffffff ffffffff ffffffff ffffffff 000919fd 86e5afce 7fc11c94} \\
& \texttt{0e0827c8 03be05bb 71f8de48 c61d6d5f 0feb036d a1ff2f8b 5f596108 3d142538}
\end{aligned}
$$

We obtain:

$$R(m_1) \cdot R(m_2) = R(m_3) \cdot R(m_4) \bmod N$$

where messages m_1, m_2, m_3 and m_4 are as small as one third of the size of the modulus.