The Padding Scheme for RSA Signatures

Lynn Margaret Batten [1]
Deakin University, Australia
lmbatten@deakin.edu.au

Christopher Wolf [2]
Ruhr-University Bochum, Germany
cbw@hgi.rub.de

This paper is dedicated to the memory of Jim Totten, a fellow student of number theory and good friend.

Abstract:
The RSA scheme is used to sign messages; however, in order to avoid forgeries, a message can be padded with a fixed string of data P. De Jonge and Chaum showed in 1985 that forgeries can be constructed if the size of P (measured in bytes) is less than the size of $N/3$, where N is the RSA modulus. Girault and Misarsky then showed in 1997 that forgeries can be constructed if the size of P is less than the size of $N/2$. In 2001, Brier, Clavier, Coron and Naccache showed that forgeries can still be constructed when the size of P is less than two thirds the size of N. In this paper, we demonstrate that this padding scheme is always insecure; however, the complexity of actually finding a forgery is $O(N)$. We then focus specifically on the next unsettled case, where P is less than $3/4$ the size of N and show that finding a forgery is equivalent to solving a set of diophantine equations. While we are not able to solve these equations, this work may lead to a break-through by means of algebraic number theory techniques.

Keywords
RSA, Cryptography, Signing, Diophantine Equation

1 RSA Fixed Padding Signature Schemes

RSA was invented in 1977 by Rivest, Shamir and Adleman [7]. It is still the most widely implemented public key scheme, and is used to provide privacy

[1]Supported by a Discovery Grant of the Australian Research Council. The author wishes to thank COSIC/ESAT at KULeuven for their hospitality, where she was a Visiting Professor.
[2]Partially supported by Concerted Research Action GOA-MEFISTO-666 of the Flemish Government (Belgium)

and authentication for digital data. Signing messages is an RSA application embedded in several standards, such as PKCS#1, v2.0 and v2.1 [8].

To sign a message m in an RSA scheme, the signer exponentiates with her private key d to get m^d and computes this modulo N, the RSA fixed modulus. To retrieve m, a receiver applies the signer's public key e to obtain $(m^d)^e \equiv m(\text{mod } N)$. The fact that applying e releases m to the receiver verifies that the owner of the key pair (d, e) was in fact the sender, as no-one else knows d.

There are many ways to attack such a signature scheme. For example, suppose Oscar is able to convince Alice to send him two different messages, m_1 and m_2, signed with Alice's private key d. Then Oscar has $(m_1)^d(m_2)^d = (m_1m_2)^d$ and can send the new message m_1m_2 to a third party, signed with Alice's key, and pretend it came from Alice. The usual way of dealing with such an attack is to allow only a certain set of *legitimate* messages (mod N) to be accepted.

A *padding scheme* fixes the set of allowed or legitimate messages modulo N to be only those values between 0 and N which have an affine form $a + wm$ for fixed, known a and w modulo N. As an example, let $N = 91$, $w = 6$ and $a = 1$. Then m can be chosen from 0 to $\lfloor 91/6 \rfloor = 15$ producing legitimate messages 1, 7, 13, 19, 25, 31, 37, 43, 49, 55, 61, 67, 73, 79, 85.

Since w^{-1} exists modulo N with very high probability (recall that in general N is a product of two very large primes), we can rewrite $a + wm$ more simply as $P + m(\text{mod } N)$ where $P \equiv aw^{-1}$ is fixed and m is bounded by the size of P. Thus, a *forgery* is a value $(P + m)^d(\text{mod } N)$ where P is fixed and m is a false message injected by an attacker, but the form and signature d appear to be legitimate.

De Jonge and Chaum [3] in Crypto'85 were the first to show that the size of P in bytes needs to be at least one third the size of N as otherwise, a forgery could be easily constructed. In 1997, Girault and Misarsky [4] were able to show that the scheme was still insecure if the size of P is less than half the size of N, again by directly constructing forgeries. Then in [2], Brier, Clavier, Coron and Naccache extended this to two thirds. In 2002, some additional forgery constructions appeared in this last case by Lenstra and Shparlinski [6]. The next case, where P is less than three quarters the size of N, remains to be solved, in terms of a direct construction.

Some recent papers have again considered this problem. Joux, Naccache and Thomé [5] use number field sieving techniques to improve the complexity of finding forgeries in the general case. More precisely, they show that computing $r'th$ roots modulo N is easier than factoring N using current methods, given access to an oracle outputting roots of the form $x + c$, for fixed c. Oracle methods are again employed in a related paper [1] which describes two new attacks

on the now defunct PKCS #1 v1.5.

In section three we prove the general result that, no matter what the size of P, a forgery is always possible within $O(N)$ computations. This in itself is often not enough to render a cryptographic scheme useless. If it is computationally infeasible to generate a forgery, then the scheme may still be usable. In section four, we illustrate this by demonstrating explicitly how construction of a forgery is equivalent to solving a dependent system of diophantine equations for the case where P is less than three quarters the size of N.

The authors wish to thank David Naccache for directing us to the problem, and the referees for their comments.

2 Forgeries

Rephrasing the ideas of Section 1, Oscar would attempt to gather a number of legitimate messages signed by Alice with her private key d : $(P+x_1)^d$, $(P+y_1)^d$ etc. where P is fixed and public, and can combine these as products or quotients to obtain

$$\frac{\prod_{i=1}^{s}(P+x_i)^d}{\prod_{i=1}^{t}(P+y_i)^d} \equiv (P+m)^d (\text{mod } N)$$

for some new message m without knowing d. He will then claim that $P+m$ came from Alice. However, this is only possible if m is in the correct range.

The Girault, Misarsky result [3] indicates that the size of P must be at least one half the size of N in bytes. In terms of comparative size of the numbers, this translates into $P > \sqrt{N}$. Since $P+m$ is a value less than N, we conclude that $m < \sqrt{N}$. The Brier, Clavier, Coron, Naccache result translates into $P > (\sqrt[3]{N})^2$ and so $m < \sqrt[3]{N}$.

In the next section, we show that for all $r \geq 2$, forgeries exist with $1 \leq m \leq \lceil \sqrt[r]{N} \rceil$. However, we do not actually construct them.

3 Forgeries Are Always Possible

As promised, we show in this section that, no matter what the size of the padding P, a forgery always exists in a fixed-pattern padding scheme. The proof is based on the pigeon-hole principle: if all values we generate are distinct, then we have too many.

THEOREM *Let P be a fixed padding for an RSA fixed-padding signature scheme with modulus N. Let r be any integer greater than or equal to two, sat-*

isfying $r - 1 < \lceil \sqrt[r]{N} \rceil$. *Then there is a message* m, $1 \leq m \leq \lceil \sqrt[r]{N} \rceil$, *such that the signature of* $P + m$ *can be forged.*

Proof. Consider the equation

$$P + x_0 \equiv \prod_{i=1}^{s} (P + x_i) \pmod{N} \tag{1}$$

where $s \geq 2, 1 \leq x_i \leq \lceil \sqrt[r]{N} \rceil$ for all $0 \leq i \leq s$, and all x_i, $1 \leq i \leq s$, are fixed and distinct. A value for x_0 in the range $[1, \lceil \sqrt[r]{N} \rceil]$ provides a forgery, either using $P + x_0$ as the forged message, or, if x_0 equals some x_i, $1 \leq i \leq s$, using a factor in the right-hand side as the forged message. (Note that $(P + x_i)^{-1}$ exists with high probability as noted earlier; in fact, only $p + q$ values are not invertible, where $N = pq$.) Clearly, $s \leq \lceil \sqrt[r]{N} \rceil$.

The plan of attack in the proof is to demonstrate that as the x_i range over their interval, then either a number of values of

$$F \equiv \prod_{i=1}^{s} (P + x_i) - P \pmod{N} \tag{2}$$

lie in the range $[1, \lceil \sqrt[r]{N} \rceil]$, giving us a forgery, or, we obtain a contradiction.

Consider two representations of the right-hand side of (2) which are equal

$$\prod_{\substack{x_i \in X \subseteq S \\ 2 \leq |X|}} (P + x_i) - P \equiv \prod_{\substack{y_i \in Y \subseteq S \\ 2 \leq |Y|}} (P + y_i) - P \tag{3}$$

where $S = \{1.2. \ldots s\}$ and whre some x_i is not equal to any y_i.

Equation (3) then results in a forgery as described in Section 2.

We may therefore assume that all values of

$$\prod_{\substack{x_i \in X \subseteq S \\ 2 \leq |X|}} (P + x_i) - P \tag{4}$$

are distinct for all subsets of S not empty and not singletons. There are $2^s - (s + 1)$ such values.

We now show that $2^s - (s + 1) > N - \lceil \sqrt[r]{N} \rceil$ if we choose s such that $s = \log_2(N)$. This will generate a contradiction, since some value of (4) must be in the range $[1, \lceil \sqrt[r]{N} \rceil]$.

If $2^s - (s+1) > N - \lceil \sqrt[r]{N} \rceil$ then certainly, $2^s \geq N - \lceil \sqrt[r]{N} \rceil + 4$ and $s \geq \log_2(N - \lceil \sqrt[r]{N} \rceil + 4)$. Thus, if we choose $\lceil \sqrt[r]{N} \rceil \geq s \geq \log_2(N)$, the strict inequality above is sastisfied. □

COROLLARY *The complexity of finding a forgery using the method of the proof of the Theorem is* $O(N - \lceil \sqrt[r]{N} \rceil) = O(N)$.

Proof. since we calculate (at most) $2^s - (s+1)$ products, as shown in the proof s is about $\log_2(N - \lceil \sqrt[r]{N} \rceil + 4)$. Thus 2^s is of order $O(N - \lceil \sqrt[r]{N} \rceil) = O(N)$. □

As r grows, the complexity approaches N rapidly which may explain why resolving the 3/4 case has proved considerably more difficult than that for 1/2 and 2/3.

EXAMPLE For $N = 1034273, r = 4, \lceil \sqrt[4]{1034273} \rceil = 36$, we have $2^{23} = 8388608$ and $2^{24} = 167772164$. So $2^s > 1034237 + (s+1)$ if $s = 24$. Thus $s = 24$ suffices to ensure a forgery in this case.

4 Constructing Forgeries

While knowing it is possible to construct forgeries is worthwhile in itself, if it is too difficult, or takes too long, to actually construct a forgery, the scheme may still be used with some sense of security. In this section, we reduce the problem of forgery construction to that of solving a dependent system of diophantine equations in the case where the size of P is less than three quarters the size of N. However, in this case, we have no general method of solving the system and leave this as an open problem.

The diophantine equations we are after are produced from the quotient equations in the previous section. A forgery results in an equality of two products simply by cross-multiplying. The number of terms on each side can be equalized simply by adding sufficient terms of the form $P + x_i = 1$.

The papers dealing with the cases one third, one half and two thirds derive their forgeries from such equations. Here we illustrate the situation for the next case, three quarters. We rewrite a message m as a sum or difference $x + y$ etc.

CASE 3/4
Consider $(P + x + y)(P + z + w)(P + v + s) \equiv (P + x - y)(P + z - w)(P + v - s) \pmod{N}$ which we want to solve for $0 < |x + y|, |x - y|, |z + w|, |z - w|, |v + s|, |v - s| < N^{1/4}$. This implies $0 < |x|, |y|, |z|, |w|, |v|, |s| < N^{1/4}$.

Expanding and multiplying by $2^{-1} \bmod N$ (N is odd), we obtain

$$P^2(y+w+s)+P(x(w+s)+z(y+s)+v(y+w))+$$
$$xzs+xwv+yzv+yws \equiv 0 \ (mod\ N) \tag{4}$$

Let $P^2 \equiv Q$, $0 < Q < N$.

By the extended Euclidean algorithm (see reference [4]), there exist t_Q and r_Q such that

$$t_Q Q \equiv r_Q \ (mod\ N),\ |t_Q| < N^{1/4}, 0 < r_Q < 2N^{3/4}.$$

And there exist t_P and r_P such that

$$t_P P \equiv r_P \ (mod\ N),\ |t_P| < N^{1/2}, 0 < r_P < 2N^{1/2}.$$

So $t_Q Q + t_P P \equiv r_Q + r_P \ (mod\ N)$.

Thus (4) becomes, for known r_Q and r_p

$$r_Q + r_P + x(zs+wv) + y(zv+ws) \equiv 0 \ (mod\ N) \tag{4}'$$

We want to obtain y, w, s, x, z and v such that

$$t_Q = y+w+s, \tag{5}$$

$$t_P = x(w+s)+z(y+s)+v(y+w) \tag{6}$$

and such that (4)' holds. Since $r_Q + r_P$ is a known quantity, we can re-write the equation (4)' with constraints as:

determine s, v, w, x, y and z such that

$$x(zs+wv) + y(zv+ws) \equiv A \ (mod\ N) \tag{4}^*$$

$$t_Q = y+w+s, \tag{5}$$

$$t_P = x(w+s)+z(y+s)+v(y+w) \tag{6}$$

where A, t_P and t_Q are known quantities, A is less than N, $0 < |x|$, $|y|$, $|z|$, $|w|$, $|v|$, $|s| < N^{1/4}$, $|t_Q| < N^{1/4}$ and $|t_P| < N^{1/2}$.

Similar systems of equations can be developed for each value of r from the preceding section, but clearly, as r increases, so does the complexity of the equations. We do not know how to solve these equations but hope to inspire these working in the field of diophantine equations to tackle them.

References

[1] A. Bauer, J. - S. Coron, D. Naccache, M. Tibouchi and D. Vergnaud, On the broadcast and validity-checking security of PKCS#1 v1.5 encryption. Proceedings of ACNS 2010, LNCS 6123, pp. 1-18.

[2] E. Brier, C. Clavier, J.-S. Coron and D. Naccache, Cryptanalysis of RSA signatures with fixed-pattern padding. Proceedings of Crypto'01, LNCS vol. 2139, Springer-Verlag 2001, pp. 433-439.

[3] W. De Jonge and D. Chaum, Attacks on some RSA signatures. Proceedings of Crypto'85, LNCS vol. 218, Springer-Verlag 1986, pp. 18-27.

[4] M. Girault and J.-F. Misarsky, Selective forgery of RSA signatures using redundancy, Proceedings of Eurocrypt'97, LNCS vol. 1233, Springer-Verlag 1997, pp. 495-507.

[5] A. Joux, D. Naccache and E. Thomé, When $e'th$ roots become easier than factoring. Proceedings of Asiacrypt 2007, LNCS 4833, pp. 13-28.

[6] A.K. Lenstra and I.E. Shparlinski, Selective forgery of RSA signatures with fixed-pattern padding, In PKC 2002, LNCS vol. 2274, Springer-Verlag 2002, pp. 228-236.

[7] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, CACM 21, 1978.

[8] RSA Laboratories, PKCS# 1: RSA cryptography specifications, version 2.0, September 1998, version 2.1, June 2002