

Analysis of Two RSA Signature Blinding Schemes

TR 99-34
October 9, 1999

Chris Hall and Bruce Schneier

Counterpane Systems
101 East Minnehaha Parkway
Minneapolis, MN 55419 (612) 823-1098
schneier@counterpane.com

Confidential — Counterpane Systems and Alkor
No use or disclosure of this information is permitted without prior written consent.

1 Introduction

We have read and reviewed the original document *Blind unanticipated RSA-signature schemes*. Overall we find the mathematics to be sound and the methods worth further consideration. We found almost no flaws in the algorithm and would encourage other people to perform separate analysis. We present our comments on Scheme 1 in Section 2. These are relatively minor comments and largely deal with implementation details.

2 Scheme 1

- Ignoring the two attacks mentioned in the original document one could choose R to be a large prime between N and $2N$. Then the number of primes in this range is asymptotic to

$$\frac{2N}{\log(2N)} - \frac{N}{\log(N)} \leq \frac{N}{\log(N)}.$$

Therefore we expect to have roughly

$$\log(N) - \log \log(N)$$

bits of entropy. The nice thing about this choice of R is that it will work for any exponent E . Of course, the downside is that one must work to find a large prime to use for blinding.

- Method 1 is really a special case of Method 2. The proper comparison for the signer to perform is

$$f(M')g(M) \equiv f(M)g(M') \pmod{N}$$

- In the test of condition (B1) the method for determining Y should be deterministic in X . That is, if the user presents the same X then she should receive the same Y from the signer. Otherwise the user may gain enough information to factor N .
- In the tests of conditions (B1), (B2), and (B3) it would be better to force the randomly chosen value to be the image of a hash. That is, the user provides a random value and the hash is used for the computation. Conventional factoring algorithms use linear algebra to determine (indirectly) the square-roots of a set of small primes. If an attacker could determine these directly then it would take one smooth number for the set of primes queried and then the attacker could factor N .
- If an attacker has two messages M_1 and M_2 which have no particular relation in $\mathbb{Z}/N\mathbb{Z}$, then one can show that given a signature for M_1 that one cannot turn this into a signature for M_2 via the blinding scheme. That is, one cannot determine an R such that

$$M_1 \equiv M_2^R \pmod{N}$$

which is what appears to be necessary to forge signatures.

3 Patents and Patentability

We know of no patents that cover the specific scheme described in the document listed above. Nor are we aware of any other cryptographer that has come up with the same scheme. There

Confidential — Counterpane Systems and Alkor

No use or disclosure of this information is permitted without prior written consent.

are other schemes for blind signatures that may be relevant prior art—schemes by David Chaum and Stefan Brands—and we recommend that you consult a patent attorney.

We believe that the scheme described in the document listed above is patentable, both in the U.S. and in other countries.

Confidential — Counterpane Systems and Alkor

No use or disclosure of this information is permitted without prior written consent.