Anderson's RSA Trapdoor Can Be Broken

Burton S. Kaliski Jr.*

February 14, 1994

Abstract

The RSA trapdoor proposed in Ross Anderson's recent letter can be broken.

A recent letter by Ross Anderson [1] proposes a "trapdoor" in the RSA public-key cryptosystem [5] whereby a hardware device generates RSA primes p and p' in such a way that the hardware manufacturer can easily factor the RSA modulus $n = pp'$. Factoring the modulus hopefully remains difficult for all other parties.

The proposed trapdoor is based on a secret value A known only to the manufacturer. For 256-bit RSA primes, the secret value A is 200 bits long. The device generates primes p of the form

$$p = rA + q = r(q, A)A + q, \tag{1}$$

where q is at most about 100 bits long, and r is 56 bits long and a function of A and q. To factor the RSA modulus $n = pp'$, the manufacturer reduces the modulus modulo A to recover the product qq', following the relationship

$$n = pp' = rr'A^2 + (rq' + r'q)A + qq'. \tag{2}$$

The 200-bit product qq' is easily factored, and the manufacturer recovers the primes p and p' according to Equation 1.

*RSA Laboratories, 100 Marine Parkway, Redwood City, CA 94065. Email address: `burt@rsa.com`.

While the trapdoor is indeed practical, it can be broken: Factoring such "trapped" moduli is easy. Let $n_0, \ldots, n_k$ be a set of such moduli, and let $r_0, r_0', \ldots, r_k, r_k'$ be the corresponding parameters from Equation 2. It is easy to show the following inequalities for the given parameter lengths:

$$\left\| r_0 r_0' \frac{n_i}{n_0} - r_i r_i' \right\| \leq 2^{-41}, \quad 1 \leq i \leq k. \tag{3}$$

Such inequalities are called "simultaneous Diophantine approximations," and they are classified as "unusually good" if the error term is less than $n_0^{-1/k}$ [3]. For the given parameter lengths, this is so when k is 13 or more.

Given a set of moduli known to have such approximations, finding the approximations is straightforward. Following techniques for breaking knapsack cryptosystems (see [2], [3], [4]), one finds a set of short vectors in the lattice generated by the basis

$$\begin{pmatrix} \lambda n_0 & 0 & 0 & \cdots & 0 \\ 0 & \lambda n_0 & 0 & \cdots & \vdots \\ \vdots & 0 & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & \lambda n_0 & 0 \\ -\lambda n_1 & -\lambda n_2 & \cdots & -\lambda n_k & 1 \end{pmatrix}, \tag{4}$$

where λ is an integer near $n_0^{-1/k}$. In most cases, the short vector

$$\begin{pmatrix} \lambda(r_1 r_1' n_0 - r_0 r_0' n_1) & \cdots & \lambda(r_k r_k' n_0 - r_0 r_0' n_k) & r_0 r_0' \end{pmatrix} \tag{5}$$

is a member of the set. The secret value A follows from $r_0 r_0'$, since, by Equation 2, the integer nearest to $n_0/(r_0 r_0')$ is A^2.

One way to overcome this attack is to assign a different secret value to each device, a precaution Anderson has suggested for another purpose. Then a user can only factor his or her own moduli. The user does not need 14 moduli to find A, however. Two prime factors p and p' suffice, since the fraction r'/r is such a good approximation to the fraction p'/p that it is guaranteed to be a convergent in the continued fraction expansion of p'/p. The user can therefore detect a trapdoor even if the device generates each modulus with a different secret value.

The manufacturer's only recourse, at least as far as the proposed trapdoor is concerned, is for the device to generate each modulus with a different secret value and to keep the prime factors secret. In such a situation, the manufacturer may as well preload the device with the primes and escrow copies—a practical "trapdoor" to which all cryptosystems, not just RSA, are vulnerable.

References

[1] Ross Anderson. A practical RSA trapdoor. *Electronics Letters*, June 1993.

[2] E.F. Brickell and A.M. Odlyzko. Cryptanalysis: A survey of recent results. *Proceedings of the IEEE*, 76:578–593, 1988.

[3] J.C. Lagarias. Knapsack public key cryptosystems and diophantine approximation. In D. Chaum, editor, *Advances in Cryptology: Proceedings of CRYPTO '83*, pages 3–23, Plenum Press, New York, 1984.

[4] A.K. Lenstra, H.W. Lenstra Jr., and L. Lovasz. Factoring polynomials with rational coefficients. *Math. Annalen*, 261:513–534, 1982.

[5] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.