A variant of Wiener's attack on RSA

Andrej Dujella, Department of Mathematics, University of Zagreb

To speed up the RSA decryption one may try to use small secret decryption exponent d. However, in 1990, Wiener [8] showed that if $d < n^{0.25}$, where $n = pq$ is the modulus of the cryptosystem, then there exist a polynomial-time attack on the RSA. Namely, in that case, d is the denominator of some convergent p_m/q_m of the continued fraction expansion of e/n, and therefore d can be computed efficiently from the public key (n, e) .

In 1997, Verheul and van Tilborg [7] proposed an extension of Wiener's attack that allows the RSA cryptosystem to be broken when d is a few bits longer than $n^{0.25}$. For $d > n^{0.25}$ their attack needs to do an exhaustive search for about $2t + 8$ bits (under reasonable assumptions on involved partial convergents), where $t = \log_2(d/n^{0.25})$. In 2004, we introduced a slight modification of the Verheul and van Tilborg attack, based on Worley's result [9, 3] on Diophantine approximations of the form $|\alpha - p/q| < c/q^2$, for a positive real number c (see [2]).

In both mentioned extensions of Wiener's attack, the candidates for the secret exponent are of the form $d = rq_{m+1} + sq_m$. All possibilities for d are tested, and the number of possibilities is roughly equal to (number of possibilities for r) $\times$ (number of possibilities for s), which is $O(D^2)$, where $d = Dn^{0.25}$. More precisely, the number of possible pairs (r, s) in Verheul and van Tilborg attack is $O(D^2A^2)$, where A is the maximum of the related partial quotients a_{m+1}, a_{m+2} and a_{m+3}, while in our variant the number of pairs is $O(D^2 \log A)$ (and also $O(D^2 \log D)$). Another modification of the Verheul and van Tilborg attack has been recently proposed in [6]. It requires (heuristically) an exhaustive search for about $2t - 10$ bits, so its complexity is also $O(D^2)$. We cannot expect drastic improvements here, since, by the main result of [5], there does not exist an attack in this class with subexponential run-time.

There are two principal methods for testing:

1) compute p and q assuming that d is the correct guess;

2) test the congruence $(M^e)^d \equiv M \pmod{n}$, say for $M = 2$.

Here we present a new idea, which is to apply "meet-in-the-middle" to this second test. Let $2^{eq_{m+1}} \bmod n = a$, $(2^{eq_m})^{-1} \bmod n = b$. Then we test the congruence $a^r \equiv 2b^s \pmod{n}$. We can do it by computing $a^r \bmod n$ for all r, sorting the list of results, and then computing $2b^s \bmod n$ for each s one at a time, and checking if the result appears in the sorted list. This decreases the run-time complexity of testings phase to $O(D \log D)$ (with the space complexity $O(D)$).

We have implemented the proposed attack (in PARI and C++), and it works efficiently for values of D up to 2^{30}, i.e. for $d < 2^{30}n^{0.25}$. For larger values of D, the memory requirements become too demanded. However, a space-time tradeoff might be possible, by using unsymmetrical variants of Worley's result (with different bounds on r and s). In that way, we expect that for 1024-bits RSA modulus n, the range in which this new method can be applied might be comparable with known attacks based on LLL-algorithm (see e.g. [1, 4]).

References

[1] D. Boneh, G. Durfee, *Cryptanalysis of RSA with private key d less than* $N^{0.292}$, Advances in Cryptology - Proceedings of Eurocrypt '99, Lecture Notes in Comput. Sci. **1952** (1999), 1–11.

[2] A. Dujella, *Continued fractions and RSA with small secret exponent*, Tatra Mt. Math. Publ. bf29 (2004), 101–112.

[3] A. Dujella, B. Ibrahimpašić, *On Worley's theorem in Diophantine approximations*, preprint.

[4] J. Hinek, On the Security of Some Variants of RSA, Ph.D. Thesis, University of Waterloo, 2007.

[5] R. Steinfeld, S. Contini, H. Wang, J. Pieprzyk, *Converse results to the Wiener attack on RSA*, Public Key Cryptography - PKC 2005, Lecture Notes in Comput. Sci. **3386** (2005), 184–198.

[6] H.-M. Sun, M.-E. Wu, Y.-H. Chen, *Estimating the Prime-Factors of an RSA Modulus and an Extension of the Wiener Attack*, Applied Cryptography and Network Security, Lecture Notes in Comput. Sci. **4521** (2007), 116–128.

[7] E. R. Verheul, H. C. A. van Tilborg, *Cryptanalysis of 'less short' RSA secret exponents*, Appl. Algebra Engrg. Comm. Computing **8** (1997), 425–435.

[8] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Inform. Theory **36** (1990), 553–558.

[9] R. T. Worley, *Estimating* $|\alpha - p/q|$, Austral. Math. Soc. Ser. A **31** (1981), 202–206.