Cryptanalysis of LUC cryptosystem with short secret exponent

Bernadin Ibrahimpašić, Pedagogical Faculty, University of Bihać

In 1978, just shortly after Diffie and Hellman proposed the first public–key exchange protocol, Rivest, Shamir and Adleman [6] proposed the first practical public–key cryptosystem, now widely known as the RSA public–key cryptosystem. The modulus n of the RSA cryptosystem is the product of two different large primes p and q. The public exponent e and the secret exponent d are related by $ed \equiv 1 \pmod{(p-1)(q-1)}$.

In 1993, Smith and Lennon [7] described a new public–key cryptosystem based on a Lucas functions. The LUC cryptosystem is a generalisation of the RSA cryptosystem to the group of elements of the form $a + \sqrt{a^2-1}$ modulo n. Public key is (n, e), where n is the product of two different large primes p and q. The number e must be chosen so it is relatively prime to $(p-1)(q-1)(p+1)(q+1)$.

The public key number e and the private key number d are related by $ed \equiv 1 \pmod{S(n)}$. There are four possible values for $S(n)$: $\operatorname{lcm}(p-1, q-1)$, $\operatorname{lcm}(p-1, q+1)$, $\operatorname{lcm}(p+1, q-1)$, $\operatorname{lcm}(p+1, q+1)$.

One of the most famous attacks on a typical RSA with small secret exponents, which is called the Wiener attack, was proposed by Wiener [9] in 1990. He showed that if $d < n^{0.25}$, then d is the denominator of some convergent p_m/q_m of the continued fraction expansion of e/n. His result is based on the classical Legendre's theorem on Diophantine approximations of the form $\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$.

In 1995, Pinch [5] extended the Wiener attack to LUC cryptosystem.

In 1997, Verheul and van Tilborg [8] extended the boundary of the Wiener attack on RSA. They propose a technique to raise the security boundary of $n^{0.25}$ with exhaustive-searching for $2t+8$ bits, where $t = \log_2 d - \log_2 n^{0.25}$. The candidates for the secret exponent d are of the form $d = rq_{m+1} + sq_m$, for some positive integers r and s.

In 2004, Dujella [3] described a modification of the Verheul and van Tilborg variant of the Wiener attack on RSA. Dujella's modifications of this attack is based on the Worley result on Diophantine approximations [10] of the form $|\alpha - a/b| < c/b^2$, for a positive real number c. The candidates for the secret exponent d are of the form $d = rq_{m+1} \pm sq_m$, for some nonnegative integers r and s.

Recently, Dujella and Ibrahimpašić [4] prove several results on connection between continued fractionsand rational approximations of the form $|\alpha - a/b| < c/b^2$, for a positive integer c.

In 1999, Boneh and Durfee [1] proposed an attack on RSA with small secret exponent d which works if $d < n^{0.292}$. While the Wiener attack uses continued fractions, the Boneh and Durfee attack is based on Coppersmith's method [2] for finding small roots to polynomial equations, which is based on the LLL–lattice reduction algorithm.

Here we consired attacks to LUC cryptosystem which use continued fractions. We extend the Dujella variant of the Wiener attack to LUC cryptosystem.We describe an algorithm for finding secret key d of the form $d = rq_{m+1} \pm sq_m$, for some nonnegative integers r and s in all four cases depending on function $S(n)$. We derive bounds for r and s using above mentioned results on Diophantine approximations [3, 4, 10].

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] D. Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, Journal of Cryptology, **10** (1997), 233–260.

[3] A. Dujella, *Continued fractions and RSA with small secret exponent*, Tatra Mt. Math. Publ. **29** (2004), 101–112.

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

[5] R. G. E. Pinch, *Extending the Wiener attack to RSA–type cryptosystems*, Electronics Letters **31** (1995), 1736–1738.

[6] R. L. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public–key cryptosystems*, Communications of the ACM **21** (1978), 120–126.
[7] P. J. Smith, G. J. J. Lennon, *LUC: a new public–key cryptosystem*, Ninth IFIP Symposium on Computer Science Security, Elseviver Science Publishers, 1993, 103–117.
[8] E. R. Verheul, H. C. A. van Tilborg, *Cryptanalysis of 'less short' RSA secret exponents*, Appl. Algebra Engrg. Comm. Computing **8** (1997), 425–435.
[9] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Inform. Theory **36** (1990), 553–558.
[10] R. T. Worley, *Estimating* $|\alpha - p/q|$, Austral. Math. Soc. Ser. A **31** (1981), 202–206.