Abstract

Comparing the security of LUC and KMOV public–key cryptosystems

Bernadin Ibrahimpašić

Pedagogical Faculty, University of Bihać, Bosnia and Herzegovina

In 1978, Rivest, Shamir and Adleman proposed the first practical public-key cryptosystem, now widely known as the RSA public-key cryptosystem. Its security is based on the assumption that it is not so difficult to find two large prime numbers, but it is very difficult to factor a large composite into its prime factorization form.

In 1991, Koyama, Maurer, Okamoto and Vanstone proposed new public-key cryptosystem based on elliptic curves. Their cryptosystem is based on the difficulty of factoring large numbers and is similar to RSA. It is generally called the KMOV public-key cryptosystem.

In 1993, Smith and Lennon 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 $a + \sqrt{a^2 - 1} \bmod n$.

A well-known attack on RSA with small secret exponent d, which is called the Wiener attack, was proposed by Wiener in 1990. He showed that using continued fractions, one can efficiently recover the secret exponent d from public key (n, e) as long as $d < n^{0.25}$. In this case d is the denominator of some convergent of the continued fraction expansion of e/n.

In 1997, Verheul and van Tilborg 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 $t = \log_2 d - log_2 n^{0.25}$.

In 2004, Dujella 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.

In 1995, Pinch extended the Wiener attack to LUC and KMOV cryptosystems. Pinch showed that LUC and KMOV cryptosystems, 1024-bit modulus n, are insecure for 256-bit d.

Ibrahimpašić extended the Dujella variant of the Wiener attack to LUC and KMOV cryptosystems. Our attack shows that LUC and KMOV cryptosystems, with 1024-bit modulus n, are insecure for 270-bit secret key d.