A MULTIFACTOR RSA-LIKE SCHEME

Nadir Murru

Università degli Studi di Trento

There exists variants of RSA scheme which exploit a modulus with more than 2 factors to achieve a faster decryption algorithm. These variants are sometimes called Multifactor RSA or Multiprime RSA. Another solution which allows to obtain even faster decryption is to use RSA-like schemes based on isomorphisms between two groups. In this talk, we present an RSA-like scheme based on the Pell conic and Rédei functions with a multifactor modulus. The scheme reaches its best efficiency advantage over RSA for high security levels, since in these cases the modulus can contain more primes. Compared to the analog schemes based on elliptic curves, as the KMOV cryptosystem, the proposed scheme is more efficient. Furthermore, a variation of the scheme with larger ciphertext size does not suffer from impossible group operation attacks, as it happens for schemes based on elliptic curves.