

The work extends the Hidden Number Problem (HNP) introduced by Boneh and Venkatesan in 1996. HNP is to find an unknown integer if several approximations of its multiples modulo N are known. New method for solving an extension of HNP (EHNP) is elaborated, taking into account the fragmentation of the information on the multiples and on the hidden number itself, as well. A real scenario application of the approach is presented - the private DSA key is extracted with the knowledge of side information on 5 signing operations. Such an information can be obtained if the signatures are generated in the unsecured environment of a Pentium 4 processor with Hyper-Threading technology.