COMPARISON STUDY ON NP-HARD PROBLEM BASED DIGITAL SIGNATURE

SCHEMES

Mohammad Ahmad Alia dr.m.alia@zuj.edu.jo

Computer Information Systems Department, Faculty of Sciences and IT, Al-Zaytoonah University of Jordan,

P.O.BOX 130, Amman 11733– Jordan

 ***Abstract*—**This paper shows the development in public-key digital signature schemes which are actually based on non deterministic polynomial mathematical hard problems (NP-Hard). In general, most of the currently used digital signature cryptosystems are computationally expensive with relatively lengthy key requirement due to the dependency on the number theory. Therefore, it’s important to study the performance of the most used digital signature schemes which are based on different mathematical hard problems that are, in some sense, difficult to solve. In the surveyed schemes, we present the powerful and practical of some public-key schemes depending on its security level and execution time.