EFFICIENT ONLINE/OFFLINE SIGNCRYPTION SCHEME

BAODIAN WEI, FANGGUO ZHANG AND XIAOFENG CHEN

1School of Information Science and Technology
Sun Yat-sen University
Guangzhou 510275, P.R. China
weibd@mail.sysu.edu.cn

2Key Laboratory of Computer Networks and Information Security
Ministry of Education
Xidian University
Xi'an 710071, China

ABSTRACT—In this paper, we propose a new signcryption scheme and its online/offline version from pairings. Based on the assumption of \( k+1 \) square roots, the scheme is proven, without random oracles, to be secure against the existential forgery under an adaptive chosen-message attack. It is also proven that its IND-CPA security also implies its IND-CCA2 security. A comparison is made with existing schemes from the viewpoint of computational cost and the size of ciphertexts.