Efficient Strong Designated Verifier Proxy Signature Scheme with Low Cost

Yan Liu*, Xiaoming Hu*, Xiaojun Zhang**, Jian Wang*, Yinchun Yang*

*School of computer and information engineering Shanghai Second Polytechnic University Shanghai, China
**Hebei Normal University of Science & Technology Hebei, China
{liuyan,xmhu}@sspu.educn, xjzhang@hevttc.edu.cn

Abstract— **Designated verifier proxy signature is a special proxy signature where only the designated verifier can verify the validity. So far, numerous strong designated verifier proxy signature (DVPST) schemes have been proposed. However, many of them have been pointed out to be vulnerable to the forgery attack or have high computational cost. In 2012, Lin et al. proposed a highly efficient and strong DVPST scheme in the random oracle model. However, in this paper, we address that Lin et al.'s strong DVPST scheme does not satisfy the unforgeability. In order to overcome this problem, based on the hardness of discrete logarithm problem, we present a new strong DVPST scheme. We also make a detail analysis and comparison on the security and efficiency with other related schemes including Lin et al.'s scheme. The analysis shows that our scheme not only has excellent performance in terms of computation cost and communication cost but also possesses unforgeability, nontransferability and privacy of signer's identity.**

Keyword— ***information security; strong designated verifier signature; proxy signature; random oracle model***

Xiaoming Hu was born in 1978.12 and received the Ph.D. degree in Department of Computer Application Technology, Shanghai Jiao Tong University in 2009, china. Now, she is a vice professor and working in School of Computer and Information, Shanghai Second Polytechnic University, Shanghai, China. Her current research interests include cryptography, information security and network security.