A NEW VERIFIABLE THRESHOLD DECRYPTION SCHEME
WITHOUT TRUSTED CENTER

XU FENG¹,², LV XIN¹, LIKUN JIA¹
¹College of Computer and Information
Hohai University
²School of Earth Sciences and Engineering
Nanjing University
Nanjing, P. R. China
e-mail: njxufeng@163.com

ABSTRACT—In the most of scenarios, the trusted center dose not existed. A new verifiable threshold decryption scheme without trusted center was proposed in this paper. In order to publicly verify the identity of decryption member, the scheme forces the member to submit a commitment at the beginning of the process. Moreover, the scheme has several advantages such as cheat-proof and dynamic member revocation.

Key Words: split key; public verification; commitment; dynamical revocation