Key Sharing Scheme based on One Weighted Threshold Secret Sharing

SeongMin Yoo*, PyungKoo Park**, JinSeop Shin*, JaeCheol Ryou *

**Department of Computer Engineering, Chungnam National University, Daejeon, Korea*

***Convergence Network Research Laboratory, ETRI, Daejeon, Korea*

mingoon@home.cnu.ac.kr, parkpk@etri.re.kr, whiter1cka@gmail.com, jcryou@home.cnu.ac.kr

***Abstract*—Secret sharing scheme is a cryptographic technology that safely manages password keys by dividing them into segments. Existing (k, n) threshold secret sharing scheme has a problem of allowing recovery of original secret information by collecting k or more random segments among divided secret information segments. To resolve such problem, this paper proposes a one weighted threshold secret sharing scheme. That is, by granting weighted value on a secret segment, original secret information cannot be recovered by collecting k or more segments, as long as the segment applied with weighted value is not included in the collection.**

***Keyword*—Secret Sharing, Key Management, Cryptography**

SeongMin Yoo is a Ph.D. candidate in the Department of Computer Engineering at Chungnam National University in Republic of Korea. He received the B.S. degree in Computer Science & Engineering from Chungnam National University in 2010, the M.S. degree in Computer Engineering from same university in 2012. Hi is interested in most aspects of information security, both theoretical and practical, and his recent research is largely about applied crypto, networks security, and cloud service security.

PyungKoo Park is a senior engineer in the Electronics and Telecommunications Research Institute in Republic of Korea. He received the B.S. degree in Computer Engineering from Korea University in 1998, the M.S. degree in Computer Science from same university in 2000, and the Ph.D. degree in Computer Network and Security System at Chungnam National University in Korea. His research interests are Internet Security and Computer Networks.

JinSeop Shin is a M.S. candidate in the Department of Computer Engineering at Chungnam National University in Republic of Korea. He received the B.S. degree in Computer Science & Engineering from Chungnam University in 2012. His research interests are Smartphone Security, Cryptanalysis and Key Management Systems. His recent research is largely about Smartphone Security(in particular security in the Android OS).

JaeCheol Ryou is a professor in the Department of Computer Engineering at Chungnam National University in Korea. He received the B.S. degree in Industrial Engineering from Hanyang University in 1985, the M.S. degree in Computer Science from Iowa State University in 1988, and the Ph.D. degree in Electrical Engineering and Computer Science from Northwestern University in 1990. His research interests are Internet Security and Electronic Payment Systems.