Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 62 (2015) 11 – 12

Procedia Computer Science

The 2015 International Conference on Soft Computing and Software Engineering (SCSE 2015)

Keynote Talk

An Introduction to Multi-trapdoor Hash Functions and It's Applications

Prof. Mukesh Singhal

Chancellor's Professor
Chair of Electrical Engineering and Computer Science (EECS)
University of California, Merced, USA

Abstract.

Trapdoor hash function is a highly useful cryptographic primitive for building a wide variety of novel signature schemes, like chameleon, online-offline, threshold, proxy, sanitizable and amortized signatures. These signature schemes form an essential part of the collection of mechanisms used for securing today's computing systems. With the advent of large-scale computing systems, like clouds, the need for building signature schemes that are both efficient and scalable has become increasingly important. This talk will discuss a cryptographic primitive, called a multi-trapdoor hash function, that is designed to address this need. The proposed hash function allows multiple entities to compute a collision with a given hash value. Using this unique property of multi-trapdoor hash functions, this talk will also present a preliminary design of aggregate signature and its application in securing clouds.

Peer-review under responsibility of organizing committee of The 2015 International Conference on Soft Computing and Software Engineering (SCSE 2015)

doi:10.1016/j.procs.2015.08.397

About Prof. Mukesh Singhal:

Mukesh Singhal is a Chancellor's Professor and Chairman of the Electrical Engineering and Computer Science at the University of California, Merced. He received a Bachelor of Engineering degree in Electronics and Communication Engineering with high distinction from Indian Institute of Technology, Roorkee, India, in 1980 and a PhD degree in Computer Science from the University of Maryland, College Park, in May 1986. From 1986 to 2001, he was a faculty in the department of Computer and Information Science at The Ohio State University, Columbus, OH. From 1998 to 2001, he served as the program director of the Operating Systems and Compilers program at the National Science Foundation. From 2001 to 2012, he was a Professor and Gartner Group endowed chair in Network Engineering in the Department of Computer Science at The University of Kentucky. His current research interests include distributed and cloud computing, mobile computing, cyber-security, and computer networks. He has published over 240 refereed articles in these areas. He is a Fellow of IEEE and he was a recipient of 2003 IEEE Technical Achievement Award. He has coauthored four books titled ``Advanced Concepts in Operating Systems", McGraw-Hill, New York, 1994, "Distributed Computing Systems", Cambridge University Press 2007, ``Data and Computer Communications: Networking and Internetworking", CRC Press, 2001, and ``Readings in Distributed Computing Systems", IEEE Computer Society Press, 1993. He has served in the editorial board of "IEEE Trans. on Dependable and Secure Computing", "IEEE Trans. on Parallel and Distributed Systems", "IEEE Trans. On Data and Knowledge Engineering", and "IEEE Trans. on Computers".