A Topologically Simple Keyed Hash Function Based on Circular Chaotic Sinusoidal Map Network

N. Jiteurtragool, P. Ketthong, C. Wannaboon, and W. San-Um

Intelligent Electronics Systems Research Laboratory

Faculty of Engineering, Thai-Nichi Institute of Technology, Bangkok, Thailand, 10250

nattagit.j@gmail.com, patinya.ket@gmail.com, chatchai.wann@gmail.com, wimol@tni.ac.th

***Abstract*—**This paper presents a new high-speed topologically-simple keyed hash function based on a sinusoidal map, which offers high-degree of chaos over most parameter space regions, and a circular network topology with eight sinusoidal maps. Hash function operations involve an initial stage when the sinusoidal map accepts input message and initial conditions, and a hashing stage when alterable-length hash values are generated iteratively. Simulations of nonlinear dynamics are described in terms of Cobweb map, Lyapunov exponent, and two-dimensional bifurcation structures. Performances are evaluated in terms of original messages and condition changes, statistical analyses, collision analyses, and speed analysis. The proposed has function offers high-speed operation of less than 2.5 ms, the mean changed probabilities fall in the region of [49.09, 50.06] which is very close to 50%, and the mean changed bit number is also close to a half of hash value length. The collision tests reveal the average mean of 1387, 1647, and 2710 for the hash values of 128, 160, and 256 bits, respectively. The collision resistance is enhanced, comparing to MD5, SHA1, and some of other chaos-based approaches.

***Keyword*— Hash function, Chaotic Sinusoidal map**

Nattagit Jiteurtragool was born in Chainat Province, Thailand in 1991. He is a 4th-year student pursuing B.Eng. in Computer Engineering from Computer Engineering Department, Faculty of Engineering, Thai-Nichi Institute of Technology (TNI). Currently, he is also a research assistant at Intelligent Electronic Research Laboratory (IES). His research interests include information security systems, cryptosystems, and artificial neural networks.

Patinya Ketthong was born in Nongkhai Province, Thailand in 1989. He is a 4th-year student pursuing B.Eng. in Computer Engineering from Computer Engineering Department, Faculty of Engineering, Thai-Nichi Institute of Technology (TNI). Currently, he is also a research assistant at Intelligent Electronic Research Laboratory (IES). His research interests include nonlinear dynamics of chaotic circuits and systems, information security systems, cryptosystems, and artificial neural networks.

Chatchai Wannaboon was born in Bangkok, Thailand in 1989. He is a 4th-year student pursuing B.Eng. in Computer Engineering from Computer Engineering Department, Faculty of Engineering, Thai-Nichi Institute of Technology (TNI). Currently, he is also a research assistant at Intelligent Electronic Research Laboratory (IES). His research interests include information security systems, chaotic system, and artificial neural networks.

Wimol San-um was born in Nan Province, Thailand in 1981. He received B.Eng. Degree in Electrical Engineering and M.Sc. Degree in Telecommunications in 2003 and 2006, respectively, from Sirindhorn International Institute of Technology (SIIT), Thammasat University in Thailand. In 2007, he was a research student at University of Applied Science Ravensburg-Weingarten in Germany. He received Ph.D. in mixed-signal very large-scaled integrated circuit designs in 2010 from the Department of Electronic and Photonic System Engineering, Kochi University of Technology (KUT) in Japan. He is currently with Computer Engineering Department, Faculty of Engineering, Thai-Nichi Institute of Technology (TNI). He is also the head of Intelligent Electronic Systems (IES) Research Laboratory. His areas of research interests are artificial neural networks, control automations, digital image processing, secure communications, and nonlinear dynamics of chaotic circuits and systems.