INTERNATIONAL CONFERENCE on RECENT ADVANCES in
PURE AND APPLIED MATHEMATICS (ICRAPAM 2017)
May 11-15, 2017, Palm Wings Ephesus Resort Hotel,
Kusadasi - Aydin, TURKEY www.icrapam.org

A Publicly Verifiable Authenticated Encryption Scheme Based on Chaotic Maps and Factoring Problems

Nedal Tahat

Department of Mathematics, Faculty of Sciences
The Hashemite University, Zarqa 13133, Jordan
nidal730@hotmail.com

Abstract: In this study, an authenticated encryption scheme with public verifiability based on chaotic maps and factoring problems is proposed. The main aim of deploying a chaos-based cryptosystem is to provide encryption with several advantages over traditional encryption algorithms such as high security, speed, and reasonable computational overheads and computational power requirements. Therefore, to enhance system security, we explore the implementation of a cryptosystem algorithm based on both cryptographic and chaotic system characteristics. We also provide security against known cryptographic attacks and discuss the performance analysis of the developed system.

Keywords: Authenticated encryption scheme, chaotic maps, factoring problem.

References:

[1] C. Tsai, C. Liu, S. Tsaur and M. Hwang, A publicly verifiable authenticated encryption scheme based on factoring and discrete logarithms. International Journal of Network Security, 2017, 19(3): 443-4480

[2] P. Horster, M. Michel and H. Peterson, "Authenticated encryption schemes with low communication costs," Electronics letters, 1994, 30(15): 1212-1213.

[3] W.-B. Lee and C.-C. Chang, "Authenticated Encryption without Using a One Way Function," *Electronics Letters*,1995,31(19):1656-1657.

[4] Y. Zheng, "Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)," *Proc. CRYPTO'97*, LNCS 1294, Springer Verlag,1997: 165-179.

[5] Y. Zheng, "Signcryption and Its Application in Efficient Public Key Solution," *Proc. Information Security Workshop* (*ISW'97*), LNCS 1397, 1998.Springer-Verlad: 291-312.

[6] C. Ma and K. Chen, "Publicly Verifiable Authenticated Encryption," *Electronics Letters*, 2003. 39(3): 281-282.

[7] S. F. Tzeng, Y. L. Tang, and M. S. Hwang, \A new convertible authenticated