Compcrypt–Lightweight ANS-Based Compression and Encryption

Seyit Camtepe, *Senior Member, IEEE*, Jarek Duda, Arash Mahboubi, Paweł Morawiecki, Surya Nepal, Marcin Pawłowski, and Josef Pieprzyk

***Abstract*— Compression is widely used in Internet applications to save communication time, bandwidth and storage. Recently invented by Jarek Duda asymmetric numeral system (ANS) offers an improved efficiency and a close to optimal compression. The ANS algorithm has been deployed by major IT companies such as Facebook, Google and Apple. Compression by itself does not provide any security (such as confidentiality or authentication of transmitted data). An obvious solution to this problem is an encryption of compressed bitstream. However, it requires two algorithms: one for compression and the other for encryption. In this work, we investigate natural properties of ANS that**

***Index Terms*— Asymmetric numeral system, compression, lightweight encryption, authentication.**

I. Introduction

A MAJORITY of Internet transmission is highly redundant. Popular video/audio streaming applications such as radio, TV, Skype/Zoom/Webex teleconferencing, Netflix/Stan entertainment providers, Facebook social platforms, medical remote diagnosis and monitoring, and remote teaching are all good