



A NEW PRIMITIVE FOR STREAM CIPHERS APPLICABLE TO PERVASIVE ENVIRONMENTS

JUN CHOI¹⁺, DUKJAE MOON¹⁺, SANGJIN LEE²⁺

¹ *Samsung Public Coporation, San 7, Geoyeo-Dong, Songpa-Gu, Seoul, Korea*
{choijun1014, [djmoon17](mailto:djmoon17@hotmail.com)}@hotmail.com

² *Center for Information Security Technologies, Korea University,*
1-5ka, Anam-dong, Sungbuk-ku, Seoul, Korea
sangjin@korea.ac.kr

ABSTRACT—Computing devices in pervasive environments have limitations on the following attributes: calculation capacity, power consumption, and chip size. The huge amount of operation required for applications of cryptographic primitives restricts the implementation of these primitives in pervasive environments. In order to overcome such limitations, we propose a new primitive for stream ciphers called PC-AddRotR (Pervasive Computing - Adder Right Rotation). PC-AddRotR is easily implemented by light-weight hardware and fast word-based software. PC-AddRotR efficiently generates sequences of long period and multi-bit sequences. In addition, using a word-based adder with a nonlinear property, it has more resistance against algebraic attacks, which are known to be the strong analysis methods for stream ciphers.