AAβ-Cryptosystem: a chaos based public key cryptosystem

ABSTRACT

We describe the AAβ-cryptosystem, a new public key cryptosystem that is built by utilizing the classical one-way chaotic beta-transformati on mapping given by by fβ=βx (mod 1). The AAb-cryptosystem represents its private keys as a vector dA and uses the parallelogram law to prove that encryption and decryption does indeed occur. The mathematical hard problem for this system is likely to be harder than the classical Discrete Log Problem and to some extent probably equal or slightly better than the Elliptic Curve Discrete Log Problem (ECDLP). With the correct choice of a, β and generator point X(0), the generator point X(0)when iterated via the AAB function will have an order (i.e. period/cycle) of 2k-1 wheris the length of the private key. Because of this fact, the AAβ-Cryptosystem maybe more secure than the Elliptic Curve Cryptosystem (ECC).

Keyword: Beta-transformation; Chaotic map; Asymmetric cryptography