Investigation of the Cryptographic Applications of a Recurrence Relation Through Elliptic Curves and Collatz Conjecture

Sahin, Huseyin (School: Uskudar American Academy)

In this study, a linear recurrence relation, a(n)=a(n-1)+ (a(n-1) mod m) where m is any odd positive integer, is investigated for potential applications in cryptography. The periodic sequence is reformulated, using the characteristic polynomial, in terms of the index n and the period length T. The recurrence relation is then reformulated based on Collatz conjecture, and utilizing the progression of the sequence, an encryption/decryption protocol is developed to enhance the security level of ElGamal encryption algorithm. Runtimes and security levels are compared. The progression of the sequence is represented with card shuffling, and using the protocol, a card trick is developed. By transforming the formula of the original sequence, elliptic curves are generated using the curve fit function from scipy library, optimize module. Using the elliptic curves as the key, another cryptographic protocol is developed based on the scalar point multiplication property of elliptic curves. The algorithm is expected to be more secure than the conventional elliptic curve algorithms with a slight increase in runtime. Limitations of the proposed cryptographic applications along with their implementations are presented in the study. Finally, how to utilize lattices with the sequence for a post-quantum cryptography algorithm is suggested, where the first period of the sequence can be used to find base vectors, and by projection to create an orthogonal lattice so that the shortest vector problem can be utilized. Overall, utilizing the sequence, the security level of algorithms that are based on the same cryptography problems is improved in the mentioned algorithms.

Awards Won: