On the sequences ri, si, ti ∈ ℤ related to extended Euclidean algorithm and continued fractions

ABSTRACT

The extended Euclidean Algorithm is a practical technique used in many cryptographic applications, where it computes the sequences ri, si, ti ∈ ℤ that always satisfy ri = si a+ tib. The integer ri is the remainder in the ith sequences. The sequences si and ti arising from the extended Euclidean algorithm are equal, up to sign, to the convergents of the continued fraction expansion of a/b. The values of (ri, si, ti) satisfy various properties which are used to solve the shortest vector problem in representing point multiplications in elliptic curves cryptography, namely the GLV (Gallant, Lambert & Vanstone) integer decomposition method and the ISD (integer sub decomposition) method. This paper is to extend the proof for each of the existing properties on (ri, si, ti). We also generate new properties which are relevant to the sequences ri, si, ti ∈ ℤ. The concepts of Euclidean algorithm, extended Euclidean algorithm and continued fractions are intertwined and the properties related to these concepts are proved. These properties together with the existing properties of the sequence (ri, si, ti) are regarded as part and parcel of the building blocks of a new generation of an efficient cryptographic protocol.

Keyword: Extended Euclidean algorithm; ri, si, ti ∈ ℤ; Cryptographic