

Cryptographic applications of weak restricted integer compositions

Gustavo Zambonin

Abstract

A weak composition of an integer s is a sequence of non-negative integers, called parts, that sum to s . It is called a weak t -composition if it has exactly t parts, and n -restricted if every part is at most n . Such restricted compositions arise in constant-sum encodings for the Winternitz one-time signature scheme. Compared with the usual base- w encoding, this approach can reduce signature sizes and the costs of key generation and signature verification, but signature generation becomes more expensive because a message digest must be mapped to a composition by an unranking algorithm. We describe this cryptographic application and present an improved lexicographic unranking method that reuses partial inclusion-exclusion terms instead of recomputing the relevant composition counts. Implementations using arbitrary-precision arithmetic illustrate both the resulting speedup and the remaining cost of constant-sum encoding.