

CRYPTOGRAPHIC APPLICATIONS OF RESTRICTED INTEGER COMPOSITIONS

GUSTAVO ZAMBONIN

GUSTAVO.ZAMBONIN@POSGRAD.UFSC.BR

DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
UNIVERSIDADE FEDERAL DE SANTA CATARINA
FLORIANÓPOLIS, SANTA CATARINA, BRASIL

RESUMO. A composition of an integer s is a sequence of non-negative integers, called parts, that sum to s ; it is called t -composition if it has exactly t parts, and n -restricted if all parts are upper bounded by some integer n . Recently, there have been uses of such restricted compositions in cryptography, such as digital signature schemes and format-preserving encryption. Particularly, in the Winternitz one-time signature scheme, a *constant-sum* variant using restricted compositions (Perin et al., J. Cryptogr. Eng.) achieves lower key generation and signature verification times, and smaller signature sizes. However, the cost of signature generation is increased due to the use of unranking algorithms to encode messages to be signed. We propose improvements to such encoding algorithms, using new combinatorial objects to achieve faster unranking, as well as faster implementations of the previously published algorithms.

Key words: Integer compositions. Hash-based signatures. Unranking algorithms.