Two methods on computing $g^ah^b$ in a group.


Summary: In applied cryptography, computing the group element $g^ah^b$ is very common and very important. Especially, in the verifying step of many digital signature algorithms, the computing of $g^ah^b$ is always required. Two methods on computing $g^ah^b$ in a group are proposed in this paper. For general groups, a new left-to-right encoding algorithm, which transforms $(a, b)$ to its unsigned three-element joint sparse form, is presented. Therefore, computing $g^ah^b$ needs to scan the binary representation only once. For the groups in which computing the inverse of a given element is easy, such as elliptic curve, a method for transforming $(a, b)$ to its five-element joint sparse form is suggested. A theoretical analysis and numerical comparisons show that the developed methods are as effective as current encoding methods, but simpler than them.

Keywords: cryptography; unsigned three element joint form; five element joint sparse form