Abstract Differential power analysis (DPA) attacks can be of major concern when applied to cryptosystems that are embedded into small devices such as smart cards. To immunize elliptic curve cryptosystems (ECCs) against DPA attacks, recently several countermeasures have been proposed. A class of countermeasures is based on randomizing the paths taken by the scalar multiplcation algorithm throughout its execution which also implies generating a random binary signed-digit (BSD) representation of the scalar. This scalar is an integer and is the secret key of the cryptosystem. In this report, we investigate issues related to the BSD representation of an integer such as the average and the exact number of these representations, and integers with maximum number of BSD representations within a specific range. This knowledge helps a cryptographer to choose a key that provides better resistance against DPA attacks. Here, we also present an algorithm that generates a random BSD representation of an integer starting from the most significant signed bit. We also present another algorithm that generates all existing BSD representations of an integer to investigate the relation between increasing the number of bits in which an integer is represented and the increase in the number of its BSD representations.