Patarin, Jacques; Nachev, Valérie
Commutativity, associativity, and public key cryptography. (English) Zbl 1423.94096

Summary: In this paper, we will study some possible generalizations of the famous Diffie-Hellman algorithm. As we will see, at the end, most of these generalizations will not be secure or will be equivalent to some classical schemes. However, these results are not always obvious and moreover our analysis will present some interesting connections between the concepts of commutativity, associativity, and public key cryptography.

For the entire collection see [Zbl 1384.94004].

MSC:
94A60 Cryptography
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)

Keywords:
Diffie-Hellman algorithms; Chebyshev polynomials; new public key algorithms

Full Text: DOI