Vojvoda, Milan
Cryptanalysis of one hash function based on quasigroup. (English) Zbl 1114.94015

Summary: We discuss to what extent hash functions proposed in J. Dvorský, E. Ochodková and
Czech), Hash functions based on large quasigroups, Proc. of Velikonoční kryptologie, Brno, 1–8 (2002)]
and defined on quasigroups, are resistant to several kinds of attacks. We present an attack against these
hash functions for some special quasigroups. In details we analyze the quasigroup of modular subtraction,
which is mainly in question. Some further practical considerations will be given, too.

MSC:
94A60 Cryptography
68P25 Data encryption (aspects in computer science)

Keywords:
hash function; quasigroup; cryptanalysis