1067-Z1-2402 **Imre Tuba*** (ituba@mail.sdsu.edu), San Diego State University, Imperial Valley, 720 Heber Ave, Calexico, CA 92231, and **Jonathan Boiser** (jboiser@ucmerced.edu), School of Natural Sciences, University of California, Merced, 5200 North Lake Road, Merced, CA 95343. *Braid group cryptography and some related computational problems.*

In public key cryptography based on braid groups, A and B choose elements of the braid group B_n as their private and public keys, then use these to generate symmetric private keys for some sufficiently strong conventional cryptographic protocol. The protocol is secure if there is no computationally efficient algorithm to recover private keys from the public keys. The braid group is a group that is easy enough to describe, yet presents a number of computationally intensive challenges, such as the word and the conjugacy search problems, that can be exploited to construct key-exchange protocols that are difficult to attack. The security of such protocols depends on the difficulty of the related computational problems in the braid group, which are also of interest in their own right and are subjects of active research.

We introduce some braid-based key exchange protocols and the related computational problems. We discuss how hard these computations really may be, and present some of the ideas and algorithms that arose in the process of trying to find efficient solutions for them. We also give a brief overview of the current state of research. (Received September 23, 2010)