1148-94-47 **Matvei Kotov**, **Anton Menshov** and **Alexander Ushakov***, Castle Point on Hudson, Stevens Institute of Technology, Hudson, NJ 07030. *An attack on the Walnut digital signature algorithm.*

We analyze security properties of the WalnutDSA, a digital signature algorithm recently proposed by I. Anshel, D. Atkins, D. Goldfeld, and P. Gunnels, that has been accepted by the National Institute of Standards and Technology for evaluation as a standard for quantum-resistant public-key cryptography. At the core of the algorithm is an action, named E-multiplication, of a braid group on some finite set. The protocol assigns a pair of braids to the signer as a private key. A signature of a message m is a specially constructed braid that is obtained as a product of private keys, the hash value of m encoded as a braid, and three specially designed cloaking elements.

We present a heuristic algorithm that allows a passive eavesdropper to recover a substitute for the signer's private key by removing cloaking elements and then solving a system of conjugacy equations in braids. Our attack has 100% success rate on randomly generated instances of the protocol. It works with braids only and its success rate is not affected by a choice of the base finite field. (Received January 18, 2019)