Shpilrain, Vladimir

Cryptanalysis of Stickel's key exchange scheme. (English) Zbl 1142.94360

Hirsch, Edward A. (ed.) et al., Computer science – theory and applications. Third international computer science symposium in Russia, CSR 2008 Moscow, Russia, June 7–12, 2008. Proceedings. Berlin: Springer (ISBN 978-3-540-79708-1/pbk). Lecture Notes in Computer Science 5010, 283-288 (2008).

Summary: We offer cryptanalysis of a key exchange scheme due to *E. Stickel* ["A new method for exchanging secret keys", in: Proceedings of the third international conference on information technology and applications, ICITA 2005, IEEE Computer Society, No. 2, 426–430 (2005)], which was inspired by the well-known Diffie-Hellman protocol. We show that Stickel's choice of platform (the group of invertible matrices over a finite field) makes the scheme vulnerable to linear algebra attacks with very high success rate in recovering the shared secret key (100% in our experiments). We also show that obtaining the shared secret key in Stickel's scheme is not harder for the adversary than solving the decomposition search problem in the platform (semi)group.

For the entire collection see [Zbl 1136.68005].

MSC:

94A60 Cryptography

Full Text: DOI