Magliveras, Spyros S.; Svaba, Pavol; van Trung, Tran; Zajac, Pavol
On the security of a realization of the cryptosystem MST₃. (English) Zbl 1240.94081

Summary: A new type of public key cryptosystem called MST₃ has been recently developed on the basis of logarithmic signatures and covers of finite groups. Suzuki 2-groups have been suggested for a possible realization of the generic version of MST₃. On the one hand, due to their structure, Suzuki 2-groups allow to study the security of the system; on the other hand, they possess a simple representation allowing for an efficient implementation of the system.

In this paper, we present a detailed study of the security of this realization of MST₃. We prove a new general lower bound for the work effort required to determine the secret key in terms of the size of the underlying groups. This bound has size \( q = 2^m \), where \( q \) is the order of the finite field \( F_q \), on which the Suzuki 2-group \( A(m, \theta) \) is defined. Further, by exploiting properties of the group operation in Suzuki 2-groups, as well as a special property of canonical transversal logarithmic signatures for elementary abelian 2-groups, we show that canonical transversal logarithmic signatures are unfit for the use in this realization of MST₃.

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

Keywords:
public-key cryptosystem; logarithmic signature; random cover; Suzuki 2-group cryptanalysis; MST₃