Gong, Zheng; **Huang, Zheng**; **Qiu, Weidong**; **Chen, Kefei**
Transitive signature scheme from LFSR. (English) Zbl 1238.94033
JISE, J. Inf. Sci. Eng. 26, No. 1, 131-143 (2010).

Summary: Linear feedback sequence register (LFSR) is a useful cryptographic primitive which is widely implemented in many cryptosystems to represent finite field elements with the counterparts of minimal polynomials. In this paper, an efficient transitive signature scheme from LFSR (LFSR-TS) is considered. First, two derived LFSR sequence operations are designed for LFSR-TS, which are not proposed prior to the current work. Next, the security of LFSR-TS is proven to be existentially unforgeable against the adaptive chosen-message attack in the standard model, which only requires the assumption of the discrete logarithm problem (DLP). Finally, the comparison of performances is presented amongst LFSR-TS and some related schemes.

MSC:

94A62 Authentication, digital signatures and secret sharing

Keywords:

public-key cryptography; linear feedback sequence register; graph authentication; transitive signature; provable security