1148-11-303 **László Mérai*** (laszlo.merai@oeaw.ac.at), Altenbergerstr. 69, 4040 Linz, Austria. *Random walks on elliptic curves.*

We give an overview of pseudorandom number generators (PRNGs) based on elliptic curves over finite fields. Many PRNGs are defined via a recursion law $P_n = \psi(P_{n-1})$ for some initial point $P_0 \in E$ and a rational map (morphism) $\psi : E \to E$ of the curve $E$. An example for such PRNGs is the so-called power generator, where $\psi$ is a scalar multiplication: $\psi : P \mapsto eP$ for some integer $e \geq 2$. We consider in detail the case when $\psi$ is an arbitrary endomorphism of the curve.

We present bounds on the discrepancy and linear complexity of the obtained sequences. (Received February 05, 2019)