On linear complexity profile of Edwards curve congruential generators*

László Mérai[a], **Arne Winterhof**[b]

[a]Eötvös Loránd University
merai@cs.elte.hu

[b]RICAM
arne.winterhof@oeaw.ac.at

Abstract

In 2007, Edwards introduced a new representation of elliptic curve called *Edwards curves*. For a finite field $\mathbb{F}_q$ with odd characteristic, the Edwards curve C is defined by the equation

$$x^2 + y^2 = 1 + dx^2y^2$$

where $d \neq 0, 1$. For a non-square d one can define an addition of the points of the curve. The main advantage of the Edwards curve is that there is no different formula for adding and doubling points which prevents certain side-channel attacks.

The *Edwards curve congruential generator* is defined by $w_n = x(W_n)$ where

$$W_n = G \oplus W_{n-1} = nG \oplus W_0$$

with a fixed initial value $W_0 \in C$ and fixed $G \in C$ of order t. Clearly the sequence (w_n) is t-periodic. We prove that for $N > t/2$ we have

$$L(w_n, N) \geq \min\left\{\frac{t}{8}, \frac{2N - t - 1}{6}\right\}.$$

Keywords: linear complexity, Edwards curve, elliptic curve

MSC: 11K45

*The first author is partially supported by Hungarian National Foundation for Scientific Research, Grant No. K100291, by Eötvös Loránd University and by the Momentum (Lendület) fund of the Hungarian Academy of Sciences. Both authors are partially supported by Austrian Academy of Sciences